VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

NÁVRH INFORMAČNÍHO SYSTÉMU

INFORMATION SYSTEM DESIGN

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Jan Nečas

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Miloš Koch, CSc.

SUPERVISOR

BRNO 2019

Abstrakt

Cílem této diplomové práce je navrhnout informační systém pro správu identit, který bude poskytovat správu jejich životního cyklu s napojením na personální systém. Správu oprávnění a rozhraní pro napojení systémů fungujících na architektuře rolí.

Abstract

The aim of this Master's thesis is to design an information system that will provide administration of the whole lifecycle of identities with integration to personal system. Administration of access rights and an interface for integration of any software working with roles based architecture.

Klíčové slova

Inforační systém, správa identit, nemocnice, architektra rolí, oprávnění,

Key words

Information system, identity administration, hospital, role based architecture, access rights

Bibliografická citace

NEČAS, Jan. *Návrh informačního systému* [online]. Brno, 2019 [cit. 2019-05-09]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/116573. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Miloš Koch.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne

.....

podpis studenta

Poděkování

Rád bych poděkoval vedoucímu mé diplomové práce doc. Ing. Milošovi Kochovi CSc. za cenné rady, vstřícný přístup a pomoc při zpracování diplomové práce. Dále bych rád poděkoval oponentovi RNDr. Bohuslavu Zmekovi za pomoc při návrhu a cenné rady z praxe.

OBSAH

ÚVOD 8

1 CÍL A METODIKA PRÁCE 10

2 TEORETICKÁ VÝCHODISKÁ PRÁCE 12

2.1 SHROMAŽĎOVÁNÍ INFORMACÍ 12

2.1.1 Informace 12

2.1.2 Informační zdroj 12

2.1.3 Informační systém 13

2.2 ISMS 14

2.3 IDENTITA 14

2.3.1 Identifikátory 15

2.3.2 Atributy 15

2.3.3 Ověřovací údaje 15

2.3.4 Životní cyklus identity 16

2.4 AUTENTIZACE 18

2.4.1 Autentizace něčím, co máme 18

2.4.2 Autentizace něčím, co víme 18

2.4.3 Autentizace něčím, čím jsme 19

2.4.4 Více faktorová autentizace 20

2.5 IDENTITY MANAGEMENT – SPRÁVA IDENTIT 20

2.5.1 Databáze uživatelů 20

2.5.2 Systém řízení přístupů 21

2.5.3 Provisioning systém 22

2.6 NÁSTROJE INTERSYSTEMS 23

2.6.1 Caché 23

2.6.2 Ensemble 23

2.6.3 DeepSee 24

2.7 OBJEKTOVĚ ORIENTOVANÉ MODELOVACÍ STANDARD UML 25

2.7.1 Diagram případů užití 26

2.7.2 Diagram tříd 29

2.7.3 Sekvenční diagram 31

2.8 ARCHIMATE 33
2.8.1 Úrovně architektury ArchiMate 33
3 POPIS SOUČASNÉHO STAVU 36
3.1 SLEPT ANALÝZA 36
3.1.1 Sociální faktory 36
3.1.2 Legislativní faktory 37
3.1.3 Ekonomické faktory 38
3.1.4 Politické faktory 38
3.1.5 Technologické faktory 39
3.2 ANALÝZA 7S 39
3.2.1 Strategie 40
3.2.2 Struktura 40
3.2.3 Systémy 41
3.2.4 Sdílené hodnoty 44
3.2.5 Styl 44
3.2.6 Spolupracovníci 45
3.2.7 Schopnosti 45
3.3 SWOT ANALÝZA 46
3.4 POŽADAVKY NA SYSTÉM 48
3.4.1 Technologické požadavky 48
3.4.2 Funkční požadavky 48
3.4.3 Bezpečnostní požadavky 50
4 NÁVRH ŘEŠENÍ 51
4.1 ARCHITEKTURA SYSTÉMU 51
4.2 BUSINESS VRSTVA SYSTÉMU 52
4.2.1 Případy užití 53
4.3 APLIKAČNÍ VRSTVA 67
4.3.1 Provisioning systém 67
4.3.2 Adresářová struktura 71
4.3.3 Systém řízení přístupů 73
4.3.4 Audit systému 75

4.4 TECHNOLOGICKÁ VRSTVA 76
4.4.1 Datová struktura 77
4.4.2 Technologie klientské aplikace 79
4.4.3 Napojení na zdrojové systémy 79
4.4.4 Komunikace s napojenými systémy 80
5 EKONOMICKÉ ZHODNOCENÍ 88
5.1 NÁKLADY NA SYSTÉM 88
5.2 UŠETŘENÉ NÁKLADY NASAZENÍM SYSTÉMU 89
5.3 PŘÍNOSY NEFINANČNÍHO CHARAKTERU 89
6 ZÁVĚR 91
7 SEZNAM POUŽITÝCH ZDROJŮ 92
8 SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ 96
9 SEZNAM POUŽITÝCH TABULEK 97
10 SEZNAM OBRÁZKŮ 98
11 SEZNAM PŘÍLOH 99

ÚVOD

Nacházíme se v době již dlouhotrvajícího trendu elektronizace informací a komunikace. To sebou přináší obrovské výhody, co se týče dostupnosti informací jejich důvěryhodnosti ale také jejich integrity. Každý z těchto atributů je pak v určitých oblastech, jako je například zdravotnictví otázkou života a smrti.

Stejně jako můžou takto sdílené informace pomáhat usnadňovat život a v případech ho i zachránit. Mohou stejně lehce vést, v případě neoprávněného nakládání, k naprostému opaku záměru, se kterým byly takto sdíleny. Také proto jsou kroky v rámci problematiky elektronizace prováděny s maximální rozvahou a důrazem na bezpečnost.

Uvnitř konkrétní organizace následně tyto výše popsané důvody vedou k zavádění bezpečnostní politiky pro nakládání s informacemi a komunikaci, jak vnitropodnikové tak s venkovním světem.

Zavádění bezpečnostní politiky však vypadá naprosto odlišně v rámci malé firmy o pěti zaměstnancích na rozdíl od organizace, jejíž součástí jsou tisíce zaměstnanců naprosto rozličných pracovní náplně, nebo úrovně odbornosti a odpovědnosti. To platí, obzvláště bereme-li v potaz, že v rámci dané organizace může každý uživatel plnit svoje pracovní povinnosti napříč celou škálou informačních systémů, kde každý má svůj proces poskytování informací, schvalování žádostí atd.

Ani zaváděním bezpečnostní politiky napříč informačními systémy v organizaci však práce nekončí. Často nastávají situace, které se nedají řešit obecnými pravidly, ale vyžadují individuální přístup pro daný případ. Ať už se jedná o schopného člověka který je schopen v rámci své pracovní náplně zvládnout větší rozsah než spolupracovníci, nebo například o zhrzeného zaměstnance který je odhodlaný organizaci poškodit jakýmkoliv způsobem ještě než po náhlém ukončení pracovního vztahu opustí své pracoviště.

Jako jednoduché řešení pro organizaci se jeví disponovat takovým systémem, který by byl schopný naplňovat výše zmíněné potřeby centrálně, s možností dohledání veškerých aktivit a rozhraním které umožní ostatním systémům jednoduchou integraci.

Návrh takového systému je právě obsahem této diplomové práce. Vlastní systém bude navržen dle obecně uznávaných standardů pro prostředí Fakultní nemocnice Brno, která jako přední zdravotnické zařízení v české republice a největší poskytovatel zdravotní péče na Moravě v elektronizaci rozhodně nezahálí. Historicky realizované projekty na integrační platformě InterSystems byly součástí jedené zdravotnické konference a dnes slouží jako základ pro další neméně ambiciózní projekty v oblasti ICT.

Důležité v rámci návrhu informačního systému pro jednoho konkrétního zákazníka je však mít na paměti fakt, že daný systém by neměl pouze uspokojit potřeby jednoho specifického subjektu, ale měl by spíše sloužit pro uspokojení obecných požadavků v rámci oboru a také napříč odvětvími.

1 CÍL A METODIKA PRÁCE

Cílem této práce je navrhnout informační systém pro centrální správu životního cyklu identity a jejich oprávnění jak se vyvíjí v čase. Tento systém by měl evidovat veškeré činnosti, které jeho uživatelé vykonávají stejně jako komunikaci se zdrojovými systémy a napojenými systémy.

Tento systém by měl splňovat obecně definované standardy pro správu identit, ale zároveň i uspokojit specifické požadavky daného zákazníka pro nasazení v rámci organizace.

Neméně důležité je moderní a intuitivní prostředí, které umožní jednoduchou správu bezpečnostní politiky napříč různými systémy uživatelům systému. Zároveň, ale musí splnit požadavky na funkčnost, co se individuálního nastavení týče.

Práce je dělena do čtyř základních částí. V první jsou zpracována teoretická východiska, která obecně popisují práci s informacemi, ISMS, termíny jako je Identita a její životní cyklus, autentizace, vlastní Identity management a nástroje využívané v rámci návrhu, kterými jsou nástroje Intersystems, objektově orientovaný modelovací standard UML a jazyk pro modelování architektury ArchiMate.

Druhou částí je popis současného stavu, který obsahuje analýzu vnějšího prostředí pomocí SLEPT analýzy a popis vnitřní prostředí organizace pomocí analýzy 7S. Výstupem těchto dvou analýz je analýza SWOT reflektující aktuální situaci uvnitř i vně organizace. Na závěr této kapitoly jsou analyzovány požadavky Fakultní nemocnice Brno na systém. Z technologického, funkčního a bezpečnostního hlediska.

Třetí část obsahuje vlastní návrh řešení pro daný systém. Ten se skládá z popisu architektury systému pomocí modelovacího jazyka ArchiMate. Dále je návrh dělen na 3 základní části a to business vrstvu specifikovanou pomocí případů užití, aplikační vrstvu, která popisuje vlastní složení aplikace a technologickou vrstvu popisující pomocí diagramu tříd datovou strukturu, napojení na zdrojové systémy a komunikační rozhraní s napojenými systémy.

Poslední částí je ekonomické zhodnocení, které porovnává náklady na systém a přínosy systému, které jsou nejen finančního charakteru v podobě ušetřené práce, ale také nefinančního charakteru v podobě zvýšení bezpečnosti celé organizace.

2 TEORETICKÁ VÝCHODISKÁ PRÁCE

V této části se budu popisovat teoretická východiska potřebná k pochopení dané tématiky.

2.1 Shromažďování informací

Správné shromažďování informací je jedním ze základních východisek užití ať už BI nebo jiných technik informačních technologií. Proto je důležité představit základní pojmy a přístupy.

2.1.1 Informace

*„**Informace** jsou nebytným vstupem většiny lidských činností. Většina lidských činností však také informace vytváří, ať už jako vedlejší nebo hlavní produkt, tyto informace mohou být použity jako vstupy pro jiné činnosti“* [2, s. 19].

Informace jsou data v kontextu proto je číslo (*data*) 00421915200425 užitečné člověku, který ví, že může člověku, který mu takto zanechal kontakt volat (*informace*) a ví, že 00421 je předvolba znamenající slovenského operátora (*znalost*) [3].

2.1.2 Informační zdroj

„***Informační zdrojem** budeme rozumět systém, který je reálným nebo potenciálním nositelem, zprostředkovatelem nebo šiřitelem informací. Tomuto vymezení vyhovují knihovny, databázová centra, informační střediska, televize, rozhlas apod.*“ [2, s. 22-23].

Zdroje lze dělit podle různých hledisek. Jedno z hledisek je členit zdroje podle dostupnosti na *veřejné, komerční* a *utajované*. V této práci se budeme potýkat také s problematikou soukromých informací, tedy utajovanými zdroji [2].

Při hodnocení informačního zdroje je nutné brát v potaz jeho charakteristiky. Mezi nejvýznamnější patří:

- **typ informací** udává, zda se jedná o informaci faktografickou, obrazovou nebo větu v počítačové databázi. Informační potřeba analýzy nám určuje, jaký typ informace budeme využívat,
- **rozsah** zdroje říká, kolik záznamů zdroj obsahuje. Rozsah určuje cenu informací,
- **úplnost** zdroje určuje, kolik ze všech dostupných informací, jimž se zdroj zabývá, je ve zdroji uloženo,
- **retrospektiva** udává, jak daleko do historie informace sahají,
- **perioda aktualizace** ukazuje, jak často byly do zdroje přidávány nové informace,
- **producent** spoluurčuje důvěryhodnost zdroje, je významný např. u databází,
- **dostupnost zdroje** určuje, zda je zdroj volně dostupný, dostupný pro komerční účely, nebo tajný [2].

2.1.3 Informační systém

Účelem informačního systému je zajištění správných informací na správném místě ve správný čas. Místem kam mají být informace dodány, jsou obvykle uživatelé IS a kritériem správnosti je vhodnost podpory systému v plnění jeho účelu. [4]

Pro plnění účelu informačního systému jsou důležité informační a komunikační technologie (ICT). Proto se pro informační systém podporovaný komunikačními technologiemi využívá zkratka IS/ICT. Informační a komunikační technologie jsou v kontextu informačního systému možno chápat jako hardware a software prostředky pro sběr ukládání a distribuci a vzájemnou komunikaci lidí a dílčích technologických komponent IS. [4]

Informační systém má obvykle shodný rozsah jako byznys, který monitoruje. Je však vhodné do systému zahrnout i část okolí sytému, které dodá kontext pro analýzu a doplňuje celistvost informace pro získání znalostí. Dnes je obvyklé tvořit informační systémy pro část podniku, protože i je lze brát jako samostatné celky, které je možno lehčeji zkoumat navrhovat řešení a řídit. [4]

Pro komplexní poznání informačního systému v podniku je důležité pochopení reálného postavení informačních a komunikačních technologií, které tvoří důležitý, ne však jediný formální rámec podnikových IS. [1, s. 52]

Informační systémy se v podniku nevyskytují jen v souvislosti s ICT, ale v širším rámci mohou být chápány s ohledem na míru formalizace údajů, podíl lidského faktoru i s ohledem na druh „nosičů" informací [1, s. 52]

- Informace zpracovávané prostřednictvím relační databáze a směřující k eliminaci přímé účasti člověka cestou automatizace určitých činností, sloužící k podpoře rozhodování.
- Informace uložené na dokladech, formulářích, zprávách a předpisech. Tyto informace bývají často nestrukturalizovány a obtížněji dostupné.
- Informace, které nejsou zatím zaznamenány v žádné databázi, jiné elektronické podobě, ani nejsou na žádném formuláři. Může se jednat o zkušenosti uložené v hlavách zaměstnanců, které jsou využívané operativně v okamžiku potřeby a jsou předmětem managementu znalostí. [1]

2.2 ISMS

ISMS je zkratka pro Information Security Management System, Systém řízení bezpečnosti informací česky. Jde o systematický přístup ke správě citlivých firemních informací tak, aby tyto informace zůstaly zabezpečeny. ISMS zahrnuje osoby, procesy a IT systémy [5].

2.3 Identita

Identitu lze dle M. Bishopa definovat jako souhrn atributů, které identifukjí subjekt v dané množině subjektů jednoznačně. Tato definice musí být jednoznačná a nevztahuje

se pouze na osoby, které jsou nejčastějšími nositeli identit ale také na softwarové agenty nebo hardware. [6]

Dále je možné identitu přidělit umělým objektům, jako jsou např. budovy předměty každodenní spotřeby nebo stroje. [6]

Výše zmíněná teorie je shrnuta v doporučeních organizace ITU, dle které je identita souhrnem informací o dané entitě. Tyto informace musí být dostačující pro identifikaci entity v daném kontextu. V rámci tohoto doporučení jsou definovány 3 druhy informací, ze kterých se identita skládá:

- Identifikátory,
- atributy,
- ověřovací údaje. [7]

2.3.1 Identifikátory

Identifikátor dle ITU-T Y.2720 je libovolná forma dat, užívaná pro identifikaci entity. Nejčastěji využívanými jsou čísla dokladu (občanský průkaz, cestovní pas), telefonní číslo, uživatelská jména. [7]

2.3.2 Atributy

Atributy jsou dle ITU-T Y.2720 informace, vázané k dané entitě a specifikující její charakteristiky. Pro osoby mohou být např. jméno, příjmení, pohlaví nebo datum narození. Atributy mohou být také výstupem činností entity, jako jsou tituly, role případně záznamy aktivit v rámci IS. [7]

2.3.3 Ověřovací údaje

Ověřovací údaje (credentials) jsou dle ITU-T Y.2720 definovány jako množina dat, umožňující autentizaci a autorizaci (popsané blíže v následujících kapitolách) dané entity. Mohou to být např. hesla, PIN kódy, podpisové karty atd. [7]

2.3.4 Životní cyklus identity

Systém správy identit se musí správou identit zabývat od jejich vzniku, přes údržbu až po jejich zánik. V této podkapitole budou uvedeny všechny části životního cyklu – vznik, užívání, údržba, revokace. [13]

Vznik

Vznik identity lze rozdělit na 3 části. Součástí první fáze je potvrzení atributů autoritami důvěryhodnými pro příjemce identity. V praxi to může probíhat například předložením občanského průkazu při nástupu do pracovního poměru v organizaci. [13]

Druhá fáze je přidělení ověřovacích údajů, které slouží uživateli pro autentizaci. To může proběhnout například přidělením čipové karty pro identifikaci a evidenci příchodů ke kartě může uživatel dostat ověřovací PIN, který funguje jako 2 faktory při ověření identity. [13]

Ve třetí fázi dochází k vytvoření identity složené z potvrzených atributů, ověřovacích údajů a přidělených identifikátorů. [13]

Užívání

Zavedená identita je následně využívána pro získání přístupů k požadovaným službám. Pro bezpečné nakládání s identitou existují v organizacích následující funkce. [13]

Možnost zabezpečeného vyhledání, rozlišení a autentizace ostatních identit v organizaci. Pro zajištění důvěryhodné komunikace. [13]

Možnost sdílení funkcí a atributů, které probíhá mezi poskytovateli identit a poskytovateli služeb. Tím dochází k omezení redundancí a zajištění integrity pro sdílené atributy, které mohou být umístěny v rozličných místech v systému, nebo organizace. Sdílení by mělo probíhat pouze pro ty atributy, které byly předem poskytovatelem identity, ale i jejím nositelem. [13]

Údržba

Informace o identitě se během jejího životního cyklu mění. Některé jsou měněny na základě změny životní situace např. změna příjmení žen při sňatku, nebo zdravotní stav. Jiné jsou obměňovány z bezpečnostních důvodů například hesla a digitální certifikáty. [14]

Tyto změny musí být zaznamenávány a dohledatelné pro potřeby auditu. Zároveň by však nemělo docházet k rozsáhlejším změnám kmenových identifikátorů, které je nutné vhodně zvolit, např. rodné číslo osoby nebo přidělené osobní číslo z dostatečně velké číselné řady. [14]

Revokace

Pro zajištění bezpečnosti je důležité, aby identita v systému nefigurovala déle než je nezbytně nutné. Proto je nutné, aby například v momentě ukončení spolupráce se zaměstnancem došlo k revokaci identity. Případy kdy identita přežije svého uživatele, může nastat zvýšené riziko bezpečnostních incidentů. Příkladem může být sabotáž projektu, nebo odcizení citlivých dat. [14]

2.4 Autentizace

Autentizace je úzce spojena s termínem identifikace, což je proces zjištění identity entity, kterou je třeba jednoznačně určit. Množina identifikátorů entit je zpravidla uložena v databázi. V momentě ověření uživatele jsou identifikátory poskytnuté uživatelem ověřeny proti tem uloženým v databázi. [8]

Tři základní metody autentizace lze rozdělit podle toho, že se ověřujeme: něčím co máme, co víme, čím jsme. Tyto metody budou níže přesněji popsány. [8]

2.4.1 Autentizace něčím, co máme

Metoda autentizace něčím, co máme je založena na vlastnictví určitých předmětů (tzv. tokenů). Tyto tokeny mohou mít specifické fyzické vlastnosti (např. tvar, elektrickou kapacitu), dále mohou obsahovat tajné informace (např. bezpečná hesla nebo kryptografické klíče). Některé tokeny zajišťují bezpečnost pomocí provádění specifických (obvykle kryptografických) výpočtů [9]

Výhody této metody jsou nízké požadavky na uživatele, kteří tak nejsou nuceni pamatovat si obtížná hesla, nebo jakékoliv další potřebné údaje. Jejich největším rizikem je však ztráta, nebo krádež a následné zneužití tokenu, proto je kladen důraz na jeho vysoké fyzické zabezpečení. [9]

2.4.2 Autentizace něčím, co víme

Tato forma autentizace spoléhá na to, že je uživatel schopen zapamatovat si informace, na které je v momentě autentizace dotázán. Do této skupiny informací patří například hesla jak nejrozšířenější nástroj pro autentizaci, která vynikají svým snadno pochopitelným principem. [10]

Nevýhodou hesel je nutnost spoléhat na schopnosti uživatele. V reálném provozu webu jsou nejpoužívanější hesla jednoduché fráze (heslo, pass, password), posloupnosti čísel a písmen (qwertz, 12345, abcdefgh). Pro prolomení takovýchto hesel existují programy obsahující seznam nejpoužívanějších frází (tzv. slovník), ty následně zkoušejí různé kombinace pro získání přístupu k identitě. Tento typ útoku je nazýván „Slovníkový útok“ [11]

2.4.3 Autentizace něčím, čím jsme

Poslední a téměř bezednou studnicí unikátních informací jsou biologické informace člověka, případně dalších forem života. Tato metoda je rozvíjena především pro autentizaci osob, pomocí např. otisků prstů, snímků rohovky, nebo záznamu hlasu. Autentizace osoby může probíhat například pomocí tvaru obličeje nebo chůze. [9]

Všechny biometrické autentizace řeší výskyt chyb 2 typů. Těmi jsou četnost nesprávných odmítnutí (false rejection rate - FRR) a četnost nesprávných přijetí (false acceptance rate - FAR). Oby tyto problémy nelze současně vyřešit, jelikož snížení výskytu jednoho vede k nárůstu druhého. [12]

Nesprávné odmítnutí se vyskytuje v případě odmítnutí osoby, která by přístup měla dostat. K eliminaci tohoto typu chyby stačí, když se osoba autentizuje opakovaně. Nesprávné přijetí je chyba, kdy je umožněn vstup do systému uživateli, který by ho umožněn mít neměl. Vysoká úroveň FAR je pro organizaci daleko větším bezpečnostním rizikem než FRR. Proto bývá kladen větší důraz na snížení výskytu této chyby. [11]

Výhodou biometrických skenerů je, fakt že, uživatel nepotřebuje mít při sobě žádný token ani si nemusí pamatovat jakékoliv údaje. Nevýhodou jsou vysoké náklady na pořízení forenzních systémů a nároky na provedení výpočtů. Levnější řešení provádí kontrolu s velkou chybovostí, což má velký dopad na bezpečnost a funkčnost autentizačního systému. [11]

2.4.4 Více faktorová autentizace

Z výše zmíněných metod má každá svoje nevýhody. Řešením je použití více metod pro jednu autentizaci, tak aby jedna pokryla slabé stránky té druhé. Tento systém je často využíván v případech kdy jsou kladeny vysoké nároky na zabezpečení např. ve zdravotnictví nebo bankovnictví. [11]

2.5 Identity management – správa identit

Identity management (IDM) je: „*informační systém, který dokáže z jednoho místa ovládat životní cyklus všech uživatelských účtů v organizaci a zároveň sledovat jejich změny díky auditu*“ [15]

Vlastní systém pro správu identit je složen z různých technologií, které tvoří tři hlavní pilíře IDM: databázi uživatelů, systém řízení přístupů a provisioning systém popsané podrobněji níže. [16]

2.5.1 Databáze uživatelů

Databáze uživatelů ať už je řešena jakoukoli technologií je srdcem systému správy identit. Současnými používanými řešeními jsou například Active directory pro menší organizace nebo dedikované LDAP servery pro řešení ve větších společnostech. [16]

Informace obsažené v databázi se týkají uživatelů, kteří nemusejí být jen lidé ale také další systémy hardware atd. Obsahují základní informace jako je jméno, příjmení (alternativě název systému nebo hardware), osobní číslo, heslo (často v šifrované podobě). Dále je možné uchovávat veřejné části certifikátů, fotografie a další. [16]

Databáze uživatelů jsou navrhovány a následně optimalizovány pro časté a rychlé čtení údajů, které se málokdy mění. Z důvodu zajištění vysoké dostupnosti je pro databázi důležitou funkcionalitou možnost rychlé replikace na další servery. [16]

Výše zmíněné vlastnosti poukazují na celkovou jednoduchost databáze uživatelů. Z té vyplývá, že v rámci této databáze nejsou prováděny transformace údajů ani není aplikována složitější logika, která je řízena systémem řízení přístupu. [16]

2.5.2 Systém řízení přístupů

Identita obecně slouží uživateli k získání přístupu ke službám a hardwaru, které potřebuje k vykonávání své role v organizaci. Oprávnění každého uživatele by nemělo přesahovat rámec již zmíněné role, který může být definován například náplní práce v pracovní smlouvě. [16]

Tuto funkcionalitu zabezpečuje systém řízení přístupů pomocí vykonávání centrální autentifikace, autorizace a auditu přístupů. [16]

Autentizace byla blíže popsána v kapitole 2.3. Autentizace. V rámci autentizace je možné využít Single Sign-On (SSO) umožňující výsledek autentizace využít při přístupu k různým službám (systémům) v rámci organizace. Tím bude zvýšena pohodlná práce uživatele s identitou, ale přináší také bezpečnostní rizika, nutná pro zvážení. V praxi mže SSO být realizováno při úspěšné autentizaci pomocí poskytnutí tokenu, který má danou dobu platnosti a se kterým se uživatel může přihlašovat do aplikaci využívajících stejné technologie nebo stejného autentizačního serveru. [17]

IDM může dalším aplikacím v rámci například organizace poskytnout službu přesměrování autentifikačních stánek aplikace na autentifikační server daného řešení. [16]

Autorizace zabezpečuje poskytnutí přístupu identitě ke zdrojům v rámci organizace. Systémy využívající IDM mohou řešit delegování autorizace pomocí udělování přístupu do celého systému a následně si například aplikační logiku řídit individuálně, nebo mohou využívat i řízení přístupu k jednotlivým částem aplikace. Druhý zmiňovaný způsob řešení je velice náročný na realizaci proto je možné využít kombinace výše zmíněných pomocí architektury řízení přístupu založené na rolích. [16]

RBAC – Role Based Access Control je založen na přidělování rolích jednotlivým identitám. Každá role má předem definovaná oprávnění a přístupy v aplikacích a v rámci IDM je možné tyto role pro dané systémy přidělovat identitám. [15]

Audit je poslední důležitou součástí systému řízení přístupů. Je důležité pro kvalitní IDM aby bylo evidováno, kdy byla poskytnuta práva pro danou identitu a jakému systému. Bez auditu nelze hovořit o řízená přístupů, jelikož bez něj je velmi obtížné zaručit konzistenci poskytování dat pomocí dohledání poskytovaných informací. [16]

2.5.3 Provisioning systém

Provisioning systém se obecně stará o správu databáze uživatelů. Umožňuje čerpání a aktualizaci dat ze zdrojových systémů, řídí životní cyklus identit a bezpečností politiku. [16]

Čerpání dat ze zdrojových systému je v IDM řešeno neinvazivní formou, a to bez narušení funkčnosti zdrojového systému, jelikož jako zdrojový systém často slouží personální systém organizace, který bývá od IDM oddělen. Zdrojových systémů však může být více a struktura záznamů identit proto nemusí být jednotná. Úkolem provisioning systému je udržovat jeden konstantní záznam pro všechny identity, se kterým se dále v rámci IDM pracuje. [16]

Aktualizace dat ze zdrojových systémů je spojena s řízením životního cyklu identit. Zde je kladen důraz na pokrytí všech reálných situací, kterými může identita projít. Pro osoby to může být nástup a ukončení pracovního poměru, přesun mezi organizačními jednotkami, rodičovské dovolené, stáže atd. pro systémy a hardware to mohou být mimo jiné řízené výpadky nebo poruchy. [16]

Řízení bezpečnostní politiky v provisioning systému může být realizováno pomocí přidělování rolí v systémech. Velkou část přidělování má provisioning systém možnost vykonávat automaticky, je ale důležité umožnit správci provádět změny a úpravy pro

jednotlivé identity rychle a pohodlně. To pro případ, že bude třeba zamezit jakékoliv identitě přístup do některého ze spravovaných systémů. [16]

2.6 Nástroje InterSystems

V této kapitole budou popisovány nástroje společnosti InterSystems, které poslouží v části návrhu jako prostředek pro realizaci řešení informačního systému.

2.6.1 Caché

Caché je pokročilým systémem pro správu databáze a prostředí pro rychlý vývoj aplikací. Hlavní výhodou Caché je jeho možnost škálovatelnosti, tedy řešení je možno implementovat na malý projekt, ale také projekty velkých rozměrů pracujících s Big Data. Tato nová generace databází umožňuje více způsobů přístupu k datům. Data jsou zapsána pouze jednou v podobě globálů a přístup k datům je možno realizovat pomocí objektového přístupu, vysoce výkonného SQL nebo multidimenzionálního přístupu. Všechny tyto typy přístupu se stále dotazují na stejnou datovou základnu. Součástí Caché je také několik skriptovacích jazyků a je také kompatibilní s většinou známých vývojových nástojů. [18]

2.6.2 Ensemble

Ensemble je platforma pro plynulou konektivitu a vývoj nových propojitelných aplikací. V rámci Ensemblu je možné vytvořit jednoduchou architekturu pro komunikaci aplikací a výměnu dat. Toto je možno využít např. u propojení stávajících informačních systému, které spolu nemohou jednoduše komunikovat. Pro správu komunikace slouží v Ensemble Produkce, která má tři hlavní části, těmi jsou Service (služby), Business Proces a Operation (operace). Každá z těchto částí má svoje vlastní zprávy, které automaticky vytváří a je možno v nich dohledat co se v rámci produkce odehrálo. Pro možnost správy

dílčích části produkce je možno si v kódu definovat tzv. Trace, který vypisuje požadované informace o průběhu. [18]

Services (služby)

Komunikace se zakládá na Enterprise Service Bus, toto je sběrnice napojená pomocí definovatelných vstupních adaptérů na jednotlivé informační systémy, na základě definované logiky a parametrů dokáže tvořit požadavek na sběr dat z externího systému. Tento požadavek je v rámci platformy Ensemble dále zpracováván Business procesem, který požadavek může upravovat, odesílat do dalších procesů nebo operací [18]

Opration (Operace)

Operace umožňuje zpravování požadavku a pomocí výstupního adaptéru se může také dotazovat na databáze jednotlivých externích systémů. Externí systémy tedy mohou operaci poskytovat data, tato data mohou být v operaci upravena a uložena do centrálního uložiště, nebo odeslána do další operace, která s nimi pracuje. [18]

2.6.3 DeepSee

Nástroj DeepSee jak již název napovídá, umožňuje hluboký náhled do dat. DeepSee je výkonný analytický nástroj, který umožňuje uživatelům rozhodování založená na online analýze strukturovaných a nestrukturovaných dat. Nástroj DeepSee je složen ze tří hlavních komponent. [11]

Architect

V architektu je možno vytvářet datové kostky založené na perzistentních třídách. V rámci jednotlivých kostek je možno definovat dimenze a hierarchie, různé detailní pohledy pomocí listingů, Další možností je vytvářet Subject Areas, které slouží jako omezený pohled na kostku, např. pouze část jedné dimenze atd. [11]

Analyzer

V analyzéru je možno vytvářet pohledy na data pomocí kontingenčních tabulek. Tyto tabulky mohou zobrazovat předdefinované uživatelské pohledy a agregace dat. Tento nástroj je možné využít i v rámci User Portálu pro uživatele, kteří mají s analýzou zkušenosti a vědí, jaká data je zajímají. [11]

User Portal

User Portál slouží koncovým uživatelům k zobrazování nástěnek, součástí nástěnek mohou být kontingenční tabulky, které je možno nadefinovat v Analyzéru a s tím spojené kontingenční grafy. Mimo jiné je také možno zobrazovat work-flow, Kdy jednotlivým uživatelům v rámci firemních procesů přichází úkoly k provedení, nebo kontrole na jejich vlastní nástěnky. Zde se mohou k úkolům vyjadřovat, nebo je předávat dalším úživatelům. [11]

2.7 Objektově orientované modelovací standard UML

Při objektově orientovaném modelování je v současnosti nejpoužívanější jazyk Unified Modeling Language – UML, který byl vytvořen v polovině 90. let a v současné době je považován za standart v této oblasti. Hlavní výhodou UML je nezávislost na procesu vývoje, jelikož není svázán s žádnou z konkrétních metodik. [19]

Jazyk UML umožňuje díky různým typům diagramů definovat systém z různých pohledů a s různou úrovní abstrakce. UML ve vezi 2.0 obsahuje 13 typů diagramů, které lze rozdělit na diagramy struktury a chování. [19]

Diagramy chování zachycují chování systému a patří mezi ně diagram aktivit, stavový diagram, diagram případů užití. Dále lze identifikovat interakce v systému pomocí diagramu komunikace, diagram přehledu interakcí, diagram sekvencí a diagram časování. [19]

Diagramy struktury reprezentují elementy bez závislosti na čase. Patří mezi ně diagram tříd, diagram vnitřní struktury, diagram komponent, diagram nasazení, objektový diagram, a diagram balíčků. [19]

Dále budou blíže popsány nejvýznamnější diagramy užití, tříd a sekvenční diagram. [19]

2.7.1 Diagram případů užití

Diagram případů užití (Use Case Diagram) popisuje chování systému z hlediska uživatele. V rámci diagramu případů užití jsou definovány typy uživatelů např. lidé nebo jiné systémy, které systém využívají a činnosti které vykonávají. [19]

Model případů užití se skládá z diagramů případů užití a slovních popisu pro jednotlivé případy užití. Jednotlivé případy užití vyjadřují funkční požadavky na vyvíjený systém. Prvky diagramu užití jsou aktér (Actor), případ užití (Use case) a vztah (Relation). [19]

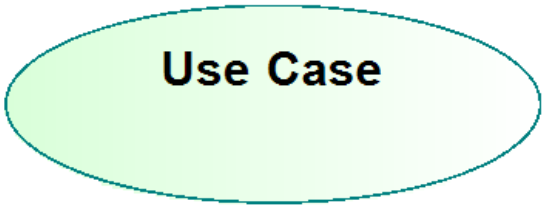
Aktér reprezentuje jednotlivé prvky z okolí systému, které se systémem komunikují. Pro aktéra neplatí, že by jím musela být živá osoba, ale může jím být i externí systém komunikující s popisovaným systémem. Aktér se v UML označuje symbolem panáčka a názem. Aktérem může být například správce systému, uživatel systému nebo napojený systém konzumující data. [19]

Aktér reprezentuje roli, kterou uživatel plní ve vztahu k popisovanému systému. Jeden uživatel může plnit více rolí a jedna role může být zároveň vykonávána více uživateli. Název aktéra by měl být podstatné jméno v jednotném čísle. Pro označování systémů, které figurují, jako aktéři je vhodné použít stereotyp <<system>>.[19]

Actor

Obr. 1 UML Aktér [vlastní zpracování]

Případ užití specifikuje část funkcionality systému, kterou může aktér plnit určitý cíl. Název případu užití by měl tento cíl vyjadřovat a je vhodné využít slovesnou vazbu, například „Založit uživatele“. Ke každému případu užití je připojen slovní popis. [19]



Obr. 2 UML Případ užití [vlastní zpracování]

Funkcionalita, která je případem užití vyjádřena se popisuje jako posloupnost interakcí mezi aktérem a systémem. Tuto posloupnost je možné označit jako scénář případu užití.

Scénář popisuje danou instanci případu a to průchod od začátku až do konce. Případ užití je spouštěn předem definovanou akcí a končí při naplnění cíle nebo při přerušení průchodu. [19]

Specifikace případu užití musí tedy obsahovat kromě základního scénáře pro úspěšný průchod i alternativní scénáře repetující chybné scénáře a variantní průchody. [19]

Struktura popisu případu užití je znázorněna v tabulce níže.

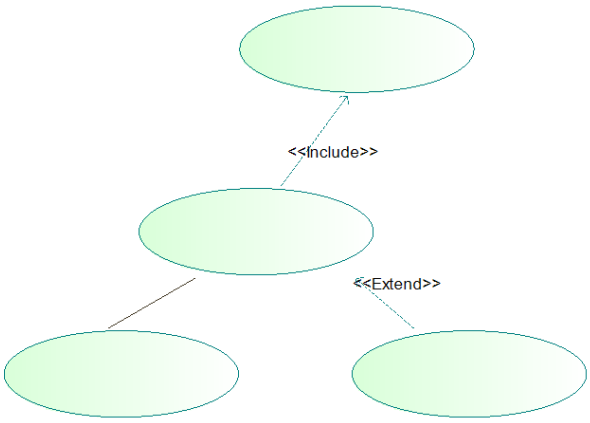
Tab. 1: Případ užití [19]

Prvek struktury popisu	Význam
Identifikace případu užití	Jednoznačné označení případu užití, UC01
Název případu užití	Srozumitelný název případu užití.
Cíl případu užití	Definování cíle, který má být pomocí případu užití splněn
Primární aktéři	Aktéři, pomocí kterých je plněn cíl případu užití
Pomocní aktéři	Aktéři, kteří poskytují službu potřebnou pro slnění úkolů primárního aktére.
Vstupní podmínky	Podmínky, které musí být splněny, pokud má být případ užití úspěšně započat
Výstupní podmínky	Podmínky, definující ukončení případu užití
Scénáře případu užití	Hlavní scénář, jenž může obsahovat alternativní scénáře obsahující výjimečné situace

Vztahy mezi případy užití se dělí na 3 základní typy.

- **Include** umožnuje do daného případu užití zahrnou jiný případ užití. Toto je možné využít například pro opakující se činnosti do samostatného případu užití. Tento případ užití se následně realizuje vždy. Může jít například o logování přístupu k danému zdroji. [19]

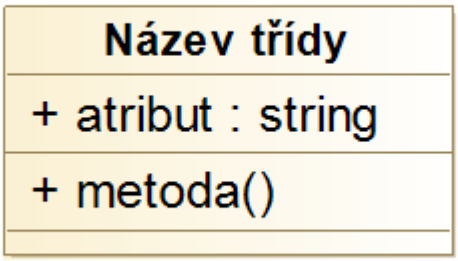
- **Extend** představuje rozšíření základního případu užití. K tomuto rozšíření dochází na pojmenovaném místě, nazývaném Extension point. Toto rozšíření je spouštěno pouze je-li splnění podmínka rozšíření. Na rozdíl od vztahu include může případ užití u vztahu extend fungovat i samostatně. Tento vztah je tedy vhodné využít při znázornění zamýšlených rozšíření systému. [19]
- **Generalize/specialize** umožňuje zachytit obecné, nebo specifické chování systému. Při jeho použití se však zhoršuje srozumitelnost modelu případů užití a proto se běžně nepoužívají. [19]



Obr. 3: UML vztahy mezi případy užití [vlastní zpracování]

2.7.2 Diagram tříd

Diagram tříd představuje statický pohled na modelovaný systém. Vyjadřuje pouze strukturu systému a nelze v něm vyjádřit interakce mezi třídami, které mezi nimi nastávají v čase. Základním prvkem je třída. Při analýze představuje třída typ objektu, který se na úrovni návrhu softwarové aplikace realizuje vytvářením konkrétních objektů. Třída vytvářející instance se nazývá konkrétní, ale ne každá třída je vytváří, proto hovoříme i o abstraktních třídách, jejichž název v UML píšeme kurzívou. [19]

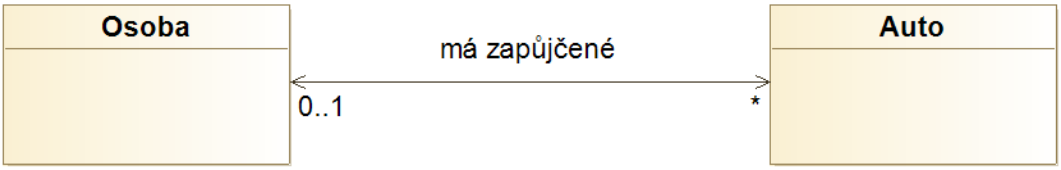


Obr. 4: UML Znázornění třídy [vlastní zpracování]

Třída se znázorňuje obdélníkem, který se skládá z 3 částí a to: název třídy jediná povinná část, atributy a metody. V systému bývá často velké množství tříd. Pro lepší přehlednost návrhu je vhodné třídy uspořádat do balíčků. [19]

Vztahy v diagramu tříd se dělí na asociace, kompozice a generalizace/specializace:

- **Asociace** modeluje spolupráci mezi třídami, při níž získává objekt referenci na jiný objekt zvenčí dočasně. Vnitřní objekt není trvale přiřazen k vnějšímu objektu, ale je spíše předán formou parametru zaslané zprávy (metody). Příkladem může být asociace mezi Osobou a Autem znázorněný na Obr. 5. [19]



Obr. 5: UML vazba tříd asociace [vlastní zpracování]

- **Kompozice** nastává v případě, že vnější objekt obsahuje vnitřní objekt jako svoji část. Čímž vnitřní objekty skládají vnější objekty. Příklad pro znázornění

představuje vztah kompozice mezi objektem Kniha a Kapitola, kde Kapitola nemůže existovat bez objektu Kniha. Vazba znázorněna na Obr. 6. [19]

Obr. 6: UML vazba tříd kompozice [vlastní zpracování]

- **Generalizace/Specializace** je druhem abstrakce, který umožňuje sdílet stejné vlastnosti a chování mezi třídami. Vztah generalizace/specializace je vztahem mezi obecnou verzí třídy a jejím speciálním případem. Umožňuje v modelování znázornit co je pro více tříd daného typu společné a co je pro ostatní specifické znázorňuje se jako speciální případ asociace 1:1. [19]

Urovně abstrakce v modelu tříd umožňuje využít různé míry detailnosti popisu pro tři základní úrovně modelu tříd – konceptuální, designovou, implementační. Při vytváření *konceptuálního* modelu tříd (ve fázi specifikace požadavků) bychom se měli zaměřit především na identifikaci odpovědnosti jednotlivých tříd. Jednotlivé odpovědnosti zaznamenáváme v doménovém modelu jako atributy. *Designový* model tříd by měl reprezentovat strukturu objektového zdrojového kódu, a proto by měl brát v potaz konkrétní konvence programovacího jazyka. *Implementační* model popisuje již technické řešení dané třídy a může sloužit jako technický popis systému. [19]

2.7.3 Sekvenční diagram

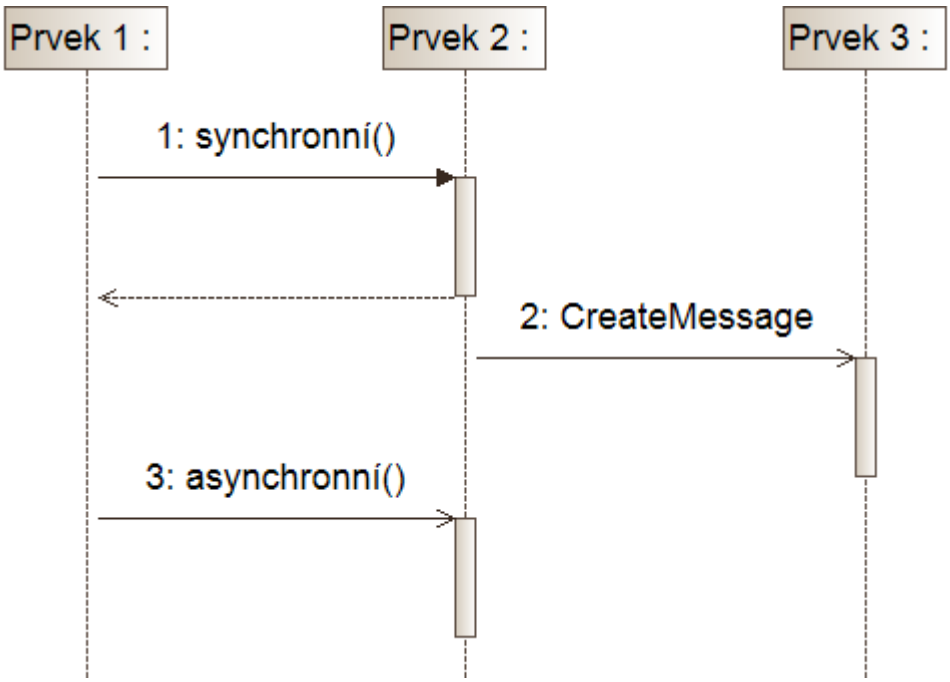
Sekvenční diagram (Sequence diagram) zachycuje grafický průběh zpracování v systému pomocí zasílání zpráv mezi jednotlivými prvky systému. Zprávy si mohou posílat objekty (ve většině případů), ale mohou komunikovat i třídy, nebo aktéři. [19]

Základní charakteristika obecného prvku v systému je schopnost přijmout zprávu a nějak na ni reagovat. U objektů může zpráva například spustit nějakou metodu, u aktéra se může jednat o postup v pracovním procesu. V rámci zpracování zprávy může prvek poslat další zprávu dalšímu prvku. Tímto vzniká sekvence zpráv reprezentovaná v sekvenčním diagramu. [19]

Prvek se zobrazuje v sekvenčním diagramu obdélníkem, ve kterém je uveden jeho název (objektu, aktéra, třídy) a svislou čarou. Zprávy se zobrazují pomocí šipky, která vede od prvku odesílajícího zprávu k prvku zprávu přijímajícímu. Zprávy jsou v sekvenčním diagramu uspořádány od levého horního rohu do pravého spodního. [19]

Zprávy mohou být dvou typů.

- Synchronní, které vyčkávají na odpověď daného systému a pokrčují v procesu až po obdržení odpovědi. Tyto zprávy označujeme plnou šipkou.
- Asynchronní, které pouze odesílají zprávu a dále se o její zpracování nezajímají. Tyto zprávy označujeme prázdnou šipkou. [19]



Obr. 7: UML sekvenční diagram zprávy [vlastní zpracování]

Při popisování chování aplikace pomocí sekvenčního diagramu lze vycházet z diagramu případu užití a scénářů případů užití, které obsahují sekvenci zpráv. U názvů prvků je vhodné uvádět typ prvku například <<actor>>, <<controller>>, <<UI>>. Zprávy, které vedou k vytvoření nebo zrušení objektu je vhodné označovat stereotypem <<create>>,<<destroy>>.[19]

2.8 ArchiMate

ArchiMate je nezávislý a otevřený modelovací jazyk pro potřeby podnikové architektury. Umožňuje její popis a vizualizaci napříč obchodními doménami jednoznačným způsobem. ArchiMate je navržen, aby reprezentoval architekturu z pohledu podnikových procesů, organizačních struktur, informačních toků vlastních systémů a technické infrastruktury. [26]

2.8.1 Úrovně architektury ArchiMate

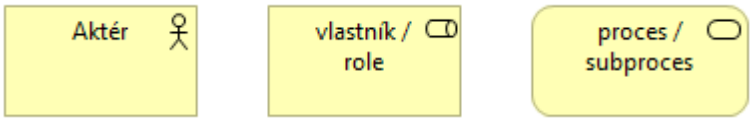
Modelování v ArchiMate se dělí do tří hlavních vrstev, kde každá reprezentuje jiné vnímání systému jako celku. Mezi výše zmiňované vrstvy patří:

- business vrstva,
- aplikační vrstva,
- technologická vrstva. [26]

Business vrstva

Business vrstva obsahuje produkty a služby poskytované systémem uvnitř organizace a externím zákazníkům. Každá ze služeb je realizována v rámci podnikových procesů, které provádí aktéři stejně jako tomu je u standardu UML. [26]

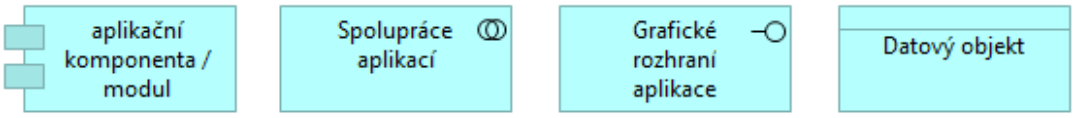
Na obrázku níže jsou zobrazeny prvky business vrstvy pro modelování aktérů provádějících činnosti v rámci jejich rolí, které mohou být vlastníkem procesu a vlastního procesu. [26]



Obr. 8: Prvky business vrstvy ArchiMate [vlastní zpracování]

Aplikační vrstva

V rámci aplikační vrstvy jsou hlavními prvky aplikační komponenty, které jsou samostatnou součástí systému a zobrazují jeho logicky oddělitelné moduly. Pomocí aplikačního rozhraní umožnují aktérům práci se systémem. Dalšími prvky jsou prvky aplikační spolupráce, které mohou být rozhraním pro komunikaci s externími systémy. Posledním popisovaným prvkem je Datový objekt, který slouží jako ekvivalent třídy v jazyce UML. [26]



Obr. 9: Prvky aplikační vrstvy ArchiMate [vlastní zpracování]

Technologická vrstva

V rámci technologické vrstvy jsou popsány služby v oblasti infrastruktury systému, které zabezpečují běh aplikací, který se realizuje pomocí infrastrukturního hardware a software. Mezi hlavní prvky patří uzel, využívaný pro medování databázových a aplikačních serverů. Zařízení je specializovaná forma uzlu pro modelování klientských aplikací. Systémový software je další specializovaná forma uzlu pro modelování programového prostředí. Infrastrukturní rozhraní slouží pro zobrazení přístupového bodu, který je zpřístupněn jiným uzlům nebo aplikačním komponentám. [26]

Obr. 10: Prvky technologické vrstvy ArchiMate [vlastní zapracovaní]

3 POPIS SOUČASNÉHO STAVU

V následující kapitole je popsán současný stav ve Fakultní nemocnici. Vnější prostředí je popsáno pomocí SLEPT analýzy, vnitřní prostředí pomocí analýzy 7S u které je kladen důraz zejména na detailní popis informačních systémů a organizační struktury. Výstupy těchto analýz budou promítnuty do SWOT analýzy. Závěrem této kapitoly je analýza požadavků Fakultní nemocnice Brno na technologie, funkčnost a bezpečnost systému.

3.1 SLEPT Analýza

SLEPT analýza se zabývá vlivem vnějších faktorů na firmu. Tudíž vlivem faktorů: Sociálních, Legislativních, Ekonomických, Politických a Technologických.

3.1.1 Sociální faktory

Sociální faktory jsou pro nemocnici jedny z nejdůležitějších. Při větším počtu obyvatel se nemocnici automaticky navyšuje počet pacientů, ať už při porodech, ošetřování pacientů dětského i dospělého věku. Z tabulky 1. můžeme pozorovat ukončení stagnace celkového počtu obyvatel města Brna a její pozvolný růst od roku 2017. Pro věkovou kategorii 0-14 let je možné pozorovat nárůst, stejně jako u kategorie 65 a více. Věkový průměr populace se pozvolna zvyšuje, což poukazuje na stárnutí populace.

Trend stárnutí populace je znatelný i ve věkové skladbě lékařských pracovníků. Toto se projevuje i v tempu vývoje nemocničních informačních systémů, které musí uspokojovat stále starší uživatele a může vytvářet napětí v rámci organizace.

Tab. 2:Počet a věkové složení obyvatel pro Brno-město.[22]

	Počet obyvatel celkem	v tom ve věku (let)			Průměrný věk
		0-14	**15-64**	**65 a více**	
2011	378 965	51 757	257 397	69 811	42,2
2012	378 327	52 615	254 105	71 607	42,3
2013	377 508	53 479	251 000	73 029	42,5
2014	377 440	54 492	248 709	74 239	42,6
2015	377 028	55 325	246 583	75 120	42,7
2016	377 973	56 413	245 178	76 382	42,8
2017	379 527	57 598	244 455	77 474	42,8

3.1.2 Legislativní faktory

Legislativně se nemocnice přímo týká povinnost vystavení receptů elektronickou formou upravovaná v rámci zákona č. č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech). [23]

A další související právní předpisy:

- *„Vyhláška č. 54/2008 Sb., o způsobu předepisování léčivých přípravků, údajích uváděných na lékařském předpisu a o pravidlech používání lékařských předpisů, ve znění pozdějších předpisů.“ [23]*
- *„Vyhláška č. 84/2008 Sb., o správné lékárenské praxi, bližších podmínkách zacházení s léčivy v lékárnách, zdravotnických zařízeních a u dalších provozovatelů a zařízení vydávajících léčivé přípravky, ve znění pozdějších předpisů.“ [23]*
- *„Vyhláška č. 236/2015 Sb., o stanovení podmínek pro předepisování, přípravu, distribuci, výdej a používání individuálně připravovaných léčivých přípravků s obsahem konopí pro léčebné použití.“ [23]*

Dále je to nový právní rámec GDPR pro ochranu osobních údajů v evropském prostoru, který má za cíl hájit práva občanů EU proti neoprávněnému zacházení s jejich daty a to včetně osobních údajů. [24]

Tato problematika se práce nemocnice přímo dotýká, jelikož pracuje nejen s osobními údaji, ale také s citlivými údaji pacientů jako můžou být výsledky psychologických vyšetření a další.

V neposlední řadě to je Evropská protipadělková směrnice, která vchází v platnost 9. 2. 2019, jejíchž obsahem je povinnost označovat léky 2D kódy. Následně při podání pacientovi pomocí načtení 2D kódu léčivo zneplatnit tak, aby s ním v rámci systému nemohlo být dále nakládáno. [25]

3.1.3 Ekonomické faktory

Nemocnice jakožto veřejná organizace je zřizovaná Ministerstvem zdravotnictví ČR. *„Základním zdrojem financování FN Brno jsou příjmy získané za poskytovanou léčebnou péči od zdravotních pojišťoven. Tyto příjmy tvoří více než* ***83 %*** *celkových výnosů FN Brno. Dalšími zdroji příjmů jsou potom tržby za prodané zboží, příjmy za léčebnou péči nehrazenou ze zdravotního pojištění atp. Provozní dotace tvoří* ***0,5 %*** *celkových příjmů FN Brno.“ [21]*

Pro rozhodování pacienta jako zákazníka není nákladnost léčby primárním kritériem, jelikož v české republice má každý občan právo na bezplatnou zdravotní péči. Proto není momentální stav ekonomiky jednoznačně možno promítnout do celkových výdajů za zdravotní péči.

Pro zacílení na pacienty, kteří jsou ochotni připlatit si vyšší péči, je důležité klást důraz na kvalitu poskytované péče a prezentaci těchto služeb nemocnice široké veřejnosti.

3.1.4 Politické faktory

Politická situace ovlivňuje Fakultní nemocnici Bohunice především tím, že je Ministerstvo Zdravotnictví ČR zřizovatelem nemocnice. *Ministerstvo zdravotnictví*

vydalo ve spolupráci se Státním zdravotním ústavem a Kanceláří Světové zdravotnické organizace (WHO) v České republice (ČR) publikaci ***„Zdraví 2020“*** [20]

Z tohoto dokumentu vyplývá strategie pro zdravotnictví, s dostatečnými zdroji financování, podporu propojení zdravotnictví napříč státy a zefektivnění poskytované péče.

3.1.5 Technologické faktory

V prostředí nemocnice je řada dostupných technologií, ale ve stále se vyvíjejícím prostředí je nutné soustředit se na možnosti inovovat reagovat na moderní trendy jak v oblasti ICT tak IS. V segmentu informačních technologií využitelných ve zdravotnictví je trendem využití čárových kódů pro sledování pacientů, léků a nemocničního vybavení. Tyto technologie umožňují lepší přehled o přímých nákladech na pacienta a navazující možnost tyto náklady řídit.

Dále s obecným rozšířením technologií do rukou široké veřejnosti se otevírají příležitosti sdílení elektronických záznamů o léčbě pacienta, nebo nákladech na jeho léčbu. S touto příležitostí jsou však svázány zvýšené požadavky na bezpečnost takto sdílených informací. Tento úkol zabezpečuje Centrum Informatiky (CI), kde jsou školení odborníci, pracující intenzivně na nejvyšší možnosti efektivity. [21]

3.2 Analýza 7S

Zatímco SLEPT analýza se zabývala vnějším prostředím firmy. Analýza 7S se zabývá vnitřním prostředím. Základních 7 kamenů této analýzy jsou: Strategie, Struktura, Systém, Sdílené hodnoty, Styl, Spolupracovníci a Schopnosti.

3.2.1 Strategie

Fakultní nemocnice v Brně definuje svoji strategii pomocí Mise, vize a hodnot, které jsou popsány níže.

Mise

FN Brno je druhým největším zdravotnickým zařízením na Moravě a druhým největším poskytovatelem zdravotních služeb na území ČR. V rámci poskytování služeb nabízí svým klientů široké spektrum specializované a super specializované péče, kterou realizuje v mnoha centrech s týmy specialistů různých odborností. Do vlastní péče přenáší výsledky vědecké a výzkumné činnosti. [21]

Vize a hodnoty

Vize FN Brno se opírá o dvě základní hodnoty, kterými jsou spokojení klienti a vzdělaní zaměstnanci. Tím směřuje k poskytování komplexní péče ve všech svých medicínských oborech. [21]

3.2.2 Struktura

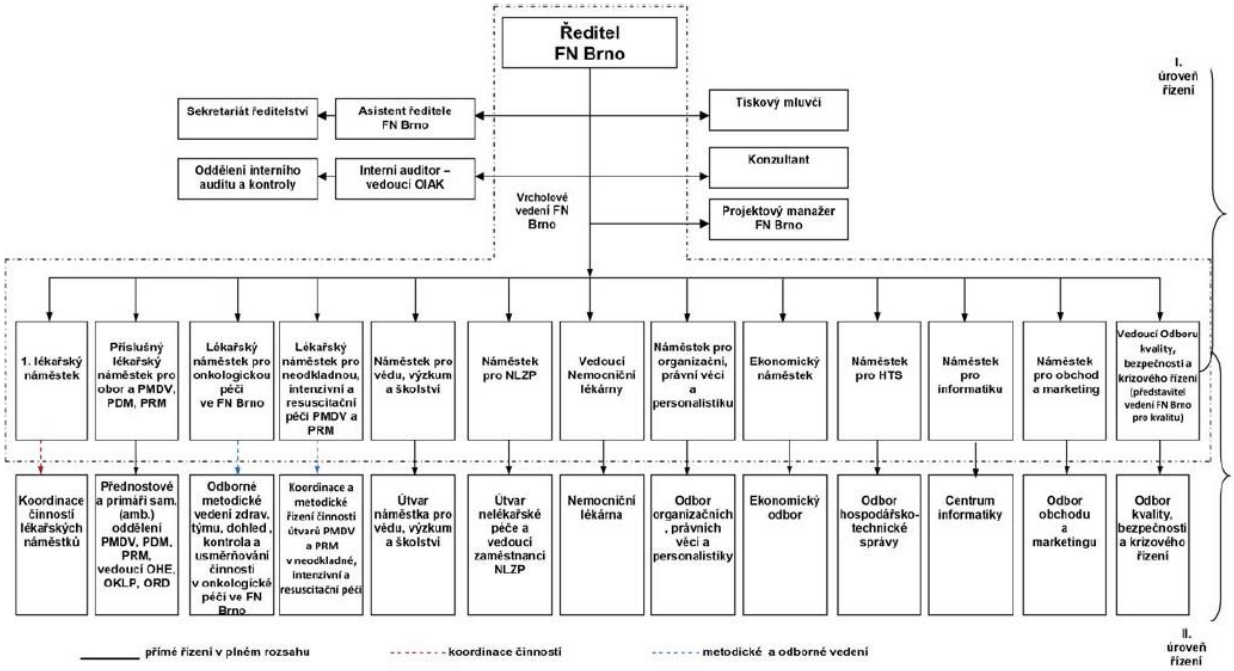
Top management nemocnice je tvořen ředitelem nemocnice a náměstky pro jednotlivá oddělení. Organizační struktura v rámci top managementu je jasně daná a řízení nemocnice má možnost jasně rozhodovat o problémech a příležitostech.

Organizační struktura v rámci různých systému uvnitř nemocnice, však není jednotná. V prostředí nemocnice jsou dvě základní organizační struktury.

Jedna pro práci v rámci medicínského informačního systému AMIS*H v rámci, které je nemocnice dělena na kliniky v rámci kterých jsou definována jednotlivá pracoviště. Jednotlivá pracoviště jsou dělena dle jejich odborností na jemnou strukturu reflektující potřeby práce s pacientem.

Druhou základní strukturou je struktura ekonomická využívána ekonomickými systémy pro sledování nákladů a personalistiku. Ta je dělena na 2 úrovně v podobě klinik a jednotlivých nákladových středisek (klinika je vlastním nákladovým střediskem). Tato struktura je však využita pro sledování nákladů v rámci celé nemocnice a to nejen nákladů na pacienta, ale také nákladů na majetek, poskytování interních služeb jako je informatika, školení, vzdělávání, dotace, studie, sponzorské dary a granty.

Tyto dvě struktury jsou do určité míry provázány, ale jejich provázání není dokonalé. Z důvodu, že některé oblasti nejsou možné reflektovat v systémech orientovaných na práci s pacientem nebo zaměstnancem.

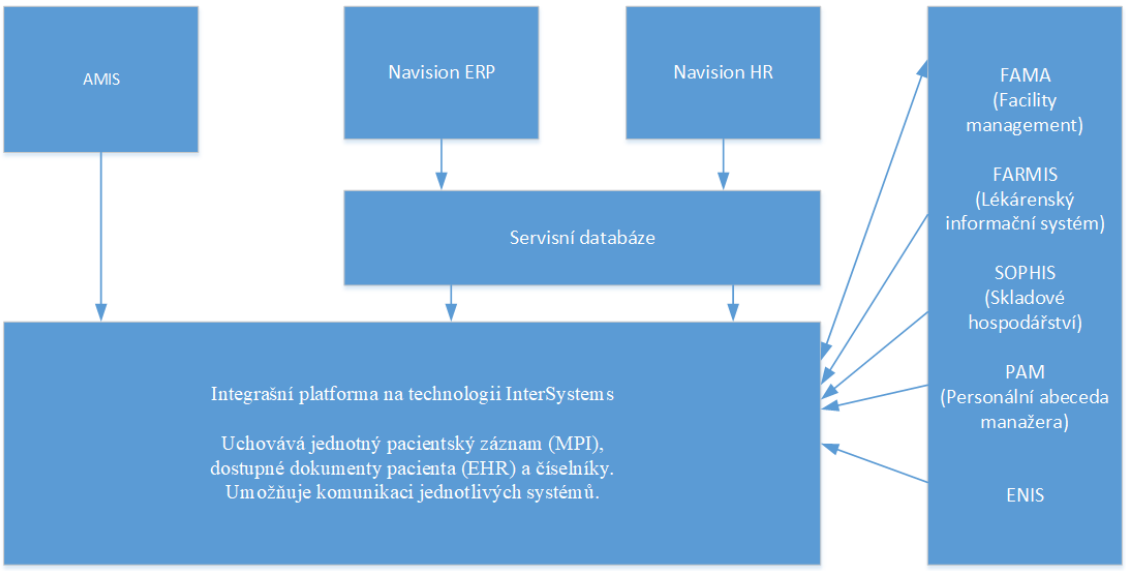


Obr. 11: Organizační struktura v rámci nemocnice [21]

3.2.3 Systémy

V rámci nemocnice je mnoho systému ekonomických, pacientských, stravovacích, docházkových atd. Tyto systémy odděleně působí v mnoha jiných nemocnicích obtíže, zvláště při potřebách komunikace jednoho s druhým. Ve fakultní nemocnici mohou tyto

systémy komunikovat přes jednotnou integrační platformu založenou na technologii společnosti InterSystems, tudíž má nemocnice možnost budovat jednotný systém a k systémům dílčím přistupovat jak individuálně tak v rámci celopodnikové koncepce.



Obr. 12: Schéma IS v rámci FN Brno [vlastní zpracování]

Pro správu klinických dat má nemocnice v současné době 3 oddělené systémy.

AMIS H

Prvním z nich je AMIS H od společnosti ICZ. Tento systém je využíván v nemocnici ve své nezměněné terminálové podobě více než 10 let. Jeho vlastnosti zatím stačily uspokojovat požadavky na provoz v rámci nemocnice. Využité technologie nejsou však modernizovány a postupně zaostávají za technologickým pokrokem. Společnost ICZ vyvinula nový produkt AMIS HD, tento produkt funguje na stejné technologii jádra a využívá novější grafické uživatelské prostředí namísto terminálového. Tato změna je pouze kosmetická a nijak neurychlí vlastní práci jádra systému, které zůstává stejné.

NAVISION HR

V rámci ekonomických informačních systému je v nemocnici nasazen NAVISION HR pro správu lidských zdrojů. V rámci tohoto systému je řízen životní cyklus zaměstnance

od jeho nástupu, změny pracovních pozic až po jeho ukončení. K tomu jsou zde zaváděny odpovídající dokumenty. V rámci personálního systému jsou vypočítávány výplaty jednotlivých zaměstnanců, jsou zde vedeny jejich pracovní úvazky.

NAVISION ERP

V rámci ekonomických informačních systému je pro sledování nákladů na jednotlivá nákladová střediska organizace nasazen systém NAVISION ERP. Ten pracuje s nákladovými středisky popisovanými v části struktury výše. Umožňuje plánování nákladů, vedení rozpočtů a v rámci integrace je napojený a integrační platformu, přes kterou je schopen komunikovat s ostatními systémy.

FAMA

Systém FAMA (Facility management) slouží pro správu majetku nemocnice od budov přes movitý majetek až po spotřební materiál. V nemocnici je nasazen za účelem kontroly schvalovacích procesů. V systému jsou žadateli zadávány žádanky na nákup a investice ty jsou následně v rámci systémového workflow schvalovány jedním nebo více schvalovateli.

Ostatní Systémy

V rámci nemocnice jsou nasazeny také další systémy: FARMIS, SOPHIS, PAM, SharePoint a další. Tyto systémy přímo nezasahují do rozsahu této analýzy, proto nebudou v této práci podrobněji popsány.

3.2.4 Sdílené hodnoty

Ve FN Brno je kladen vysoký důraz na spokojeného klienta a vzdělané zaměstnance jak již bylo zmíněno v popisu strategie výše. Podrobnější hodnoty jsou reflektovány v etickém kodexu zaměstnance FN Brno a jsou jimi:

- Klient je vždy na prvním místě.
- Personál FN Brno vykonává veškerou svou činnost s ohledem na zájmy a dobré jméno nemocnice a pacienta.
- Zaměstnanec FN Brno jedná ve shodě s obecně uznávanými mravními principy.
- Otevřenost a přátelskost vůči klientům, pacientům a jejich blízkým.
- Usilování o vysokou kvalitu a ekonomickou efektivitu veškerých činností.
- Korektní chování a rozvíjení týmové spolupráce.
- Usilování o vysokou kvalitu a ekonomickou efektivitu veškerých činností při dodržení zásad transparentnosti. [21]

Tyto hodnoty jsou obsaženy v motu nemocnice: „Žijeme pro vaše zdraví“. [21]

3.2.5 Styl

Styl práce je v úzké návaznosti na hodnoty organizace v procesu neustálého zlepšování. Jelikož je zdraví je pro člověka velmi důležité, je v rámci péče o zdraví styl klíčovým faktorem. Jedním z klíčových ukazatelů pro úspěšný styl práce je ve FN Brno úroveň komunikace. Komunikace s klientem je realizována především pomocí osobního kontaktu při vyšetřeních a pobytu v nemocnici, ale také pomocí Webových stránek, časopisů a dalších komunikačních kanálů. V rámci této komunikace v poslední době FN Brno modernizovala webové stránky tak aby odpovídaly aktuálním trendům a využívaly moderních technologií. [21]

3.2.6 Spolupracovníci

FN Brno ke konci roku 2017 zaměstnávala celkem 5 393 zaměstnanců. Z toho největším podílem 2 567 byla zastoupena skupina sanitárních zdravotních pracovníků dále 941 lékařských pracovníků a 580 technickohospodářských pracovníků. Dále jsou to také dělníci, pomocní zdravotničtí pracovníci, farmaceuti a vysokoškolští pracovníci. [21]

Zaměstnanci nemocnice jsou experty v oblastech zdravotnictví, nepostrádají však základní schopnosti práce s počítačem, nebo dostupným informačním systémem.

Z výroční zprávy je vidět že osobní náklady meziročně stoupají, což je způsobeno jak zvyšováním počtu zaměstnanců, tak i jejich vyšším platovým ohodnocením, které dosáhlo meziročně u některých kategorií až 11%. [21]

Nemocnice také disponuje centrem informatiky, kde jsou týmy odborníků, kteří se starají jak o správu nemocničních aplikací a serverů tak také vývoje.

3.2.7 Schopnosti

Neustálá snaha rozšiřování příležitostí pro vzdělávání zaměstnanců je znatelná v různých programů poskytovaných organizací svým zaměstnancům přímo, nebo zprostředkovaně pomocí externích školících programů.

Fakultní nemocnice má jako jednu ze svých základních hodnot vzdělané zaměstnance. Toho organizace dosahuje pomocí re akreditace zaměstnanců z řad lékařského i nelékařského zdravotnického personálu. Pořádáním před atestačních kurzů, adaptačních programů a školení pro zaměstnance. Další oblastí zájmu je náborová činnost, která byla v posledních letech zintenzivněna. V neposlední řadě jede o spolupráci s univerzitami. V rámci této spolupráce bylo vyřízeno 172 žádostí o poskytování informací pro studijní účely. [21]

3.3 SWOT analýza

V této podkapitole bude zpracována SWOT analýza, která bude jako zdroje využívat SLEPT analýzu a analýzu 7S. Ve SWOT matici, jsou 4 kvadranty, které obsahují každý jinou stránku organizace: silné stránky, slabé stránky, příležitosti a hrozby.

Tab. 3: SWOT analýza [vlastní zpracování]

	SILNÉ STRÁNKY **(strenghts)**	SLABÉ STRÁNKY (weaknesses)
VNITŘNÍ PROSTŘEDÍ	• Největší nemocnice na Moravě • Početné IT oddělení • Zájem vedení organizace o rozvoj IT • Dostupnost potřebných zdrojů • Zkušenosti s integračními projekty	• Vytížený personál IT a doktorů • Zastaralý informační systém nemocnice • Nedostačující znalosti v oboru IT • Dvě neprovázané organizační struktury • Nemožnost centrálně spravovat přístupová práva
VNĚJŠÍ PROSTŘEDÍ	**PŘÍLEŽITOSTI** (opportunities)	**HROZBY** (threats)
	• Možnost financování projektu v rámci naplnění národní strategie elektronizace zdravotnictví • Integrace dalších systémů na rozhraní integrační platformy • Vývoj kompozitních aplikací nad integrační platformou • Rozšíření funkcionalit integrační platformy	• Ztráta finančních prostředků v nenávratných investicích • Přílišná investice do vývoje zastaralého systému • Změna strategie nemocnice směrem od elektronizace zdravotnictví • Neoprávněný přístup ke zdrojům (aplikace, hardware, data) • Rostoucí náklady na údržbu systémů

Ze SWOT tabulky (Tab. č. 3) vyplývají následující skutečnosti:

- Organizace disponuje početným IT oddělením, pro zvládnutí otázek vnitropodnikové informatiky. Vedení i členové jednotlivých týmů má zkušenosti z předchozích integračních projektů a organizace je připravena postupovat vpřed v rozvoji propojování systému. Na tyto projekty je možné v rámci celoevropské strategie získat zdroje a realizovat je.
- Zároveň však současné projekty ve FN Brno z velké části vytěžují IT oddělení.
- Znalosti pracovníků v oblastech týkajících se specifických odborností z oboru ICT často nedostačují pro správné navržení dlouhodobých řešení pro aktuální problémy organizace.
- Mimo jiné také klinický systém provozovaný ve Fakultní nemocnici je zastaralý a přílišné investice do rozšíření tohoto systému, nebo pevné svázání nově vyvíjených systémů může v momentě výměny klinického systému, mohou mít nepříznivý vliv na cashflow organizace a hodnocení rozhodnutí vedení.
- Se zvyšujícím se počtem informačních systémů v nemocnici a jejich interních politik řízených směrnicemi nebo nastavením oprávnění se zvyšuje náročnost pro správu.
- V nemocnici chybí možnost řídit přístup k jednotlivých aplikacím z jednoho centrálního systému, který by snížil náklady na správu a umožnit audit přístupových práv.
- V neposlední řade je nutné dbát na zabezpečení veškeré komunikace týkající se pacientských dat a to ať už osobních údajů nebo záznamech o lékařských vyšetřeních.

3.4 Požadavky na systém

Daný systém by měl splňovat následující požadavky z oblasti technologických a funkčních požadavků a bezpečnostních požadavků:

3.4.1 Technologické požadavky

Obecná architektura systému by měla splňovat následující základní pilíře. Jeden pro správu organizační struktury a 3 pro právu identit a řízení přístupu

Správa organizační struktury

- **Správa organizační struktury** umožňující:
  - integraci na systémy AMIS*H a NAVISION ERP pomocí rozhraní SQL
  - sdílení informací pomocí webové služby pro softwary třetích stan.

Správa řízení přístupů

- **Databáze uživatelů -** Adresářová služba (directory service) udržuje centrální databázi uživatelů.
- **Systém řízení přístupů** - (access management) vykonává:
  - centrální autentifikaci (SSO),
  - základní autorizaci,
  - zaznamenávání (audit) přístupů
- **Provisioning systém** zabezpečuje:
  - správu databáze uživatelů,
  - její synchronizaci (s personálním systémem Navision HR),
  - řídí bezpečnostní politiku.
  - kombinaci nákladové a medicínské organizační struktury
  - řízení životního cyklu nákladových středisek a pracovišť z jednotlivých systémů

Navržený systém by měl využívat stávajících technologií již ve Fakultní nemocnici implementovaných, kterými jsou a to především integrační platformy Ensemble

3.4.2 Funkční požadavky

Níže jsou definovány strukturované požadavky na jednotlivé části systému z pohledu funkčnosti požadavků.

- **Řízení přístupů** pro:
  - **Uživatele**

        - Bez možnosti spravovat (kromě veřejných částí klíčů)
    - **Pracovní místa**
        - Obsahuje hierarchii pracovních míst
            - Lze vytvářet virtuální pracovní místa (nejsou propagovány do zdrojových systémů)
        - Umožňuje přidávat a odebírat TPM
            - Zakazovat vybrané role z TPM
        - Přidávat a odebírat Role
        - Přidávat ke speciálním rolím kompetence z předem definovaného číselníku
        - Ze zdrojového systému dopočítává zařazení na nákladové středisko
    - **Typová pracovní místa** (TPM)
        - Umožnuje vytvářet skupiny pro hromadné řízení přístupů
            - Správa práv pro lékaře, sestry, vedoucí pracovníky…
        - Možno přidělovat dle dostupných filtrů na pracovním místě.
    - **Pracovní poměry uživatele**
        - Fyzické poměry (synchronizované se zdrojovým systémem)
            - Pouze poměry s nákladovým střediskem jsou evidovány jako aktivní
            - Informace z HR NAV:
                - Jmenovka, Povolání, Úvazek, Číslo poměru
        - Virtuální poměry (vytvářené v aplikaci)
            - Mohou být na fyzickém, nebo virtuálním pracovním místě
        - *Práva na poměru:*
            - Role extra pouze pro daný poměr
            - Kompetence extra se přidává ke každé dostupné roli na poměru
            - Je možno zakazovat Role a kompetence, které byli přiřazeny na židli
    - **Role**
        - Obsahuje atribut, pro jaký Informační systém daná role existuje
        - Kompetence
    - **Kompetence**
        - Výpočtové dopočítány na židli dle hierarchie
            - UO – ke klinice
            - NS – k nákladovému středisku, které může obsahovat 1-N pracovišť
        - Statické
            - Typu ALL (ALL_ALL, UO_ALL, NS_ALL, CO_ALL)
            - Typu CO - Centra odpovědnosti leží mimo klasickou hierarchii
- **Synchronizace**
    - Prováděna v definovatelných intervalech

    - Napojena na systém
        - Navision:
            - HR
                - Informace o uživatelích
                - Pracovních poměrech
                - Pracovních místech
            - ERP
                - Informace o nákladových střediscích
        - AMIS:
            - Informace o přístupových údajích zaměstnance
            - Informace o medicínských pracovištích
- **Rozhraní viz (technická dokumentace)**
    - Webová služba poskytující informace o:
        - Volných lůžkách na pracovišti
        - Poměrech uživatele (1-N poměrů)
        - Uživateli
        - Pracovišti
        - Pracovištích na nákladovém středisku
        - Rolích uživatele
- **Způsoby napojení**
    - Napojení online
        - Napojený systém se v momentě přihlášení uživatele zeptá na aktuální role a ty si dle odpovědi webové služby aktualizuje lze využít služeb pro:
            - Role uživatele
            - Pracovní poměry uživatele
    - Napojení offline
        - Napojený systém udržuje informace o uživatelích a rolích ve své struktuře
        - V momentě změny na daném uživateli je do systému zaslána notifikace obsahující osobní číslo se změněnými přístupovými právy

3.4.3 Bezpečnostní požadavky

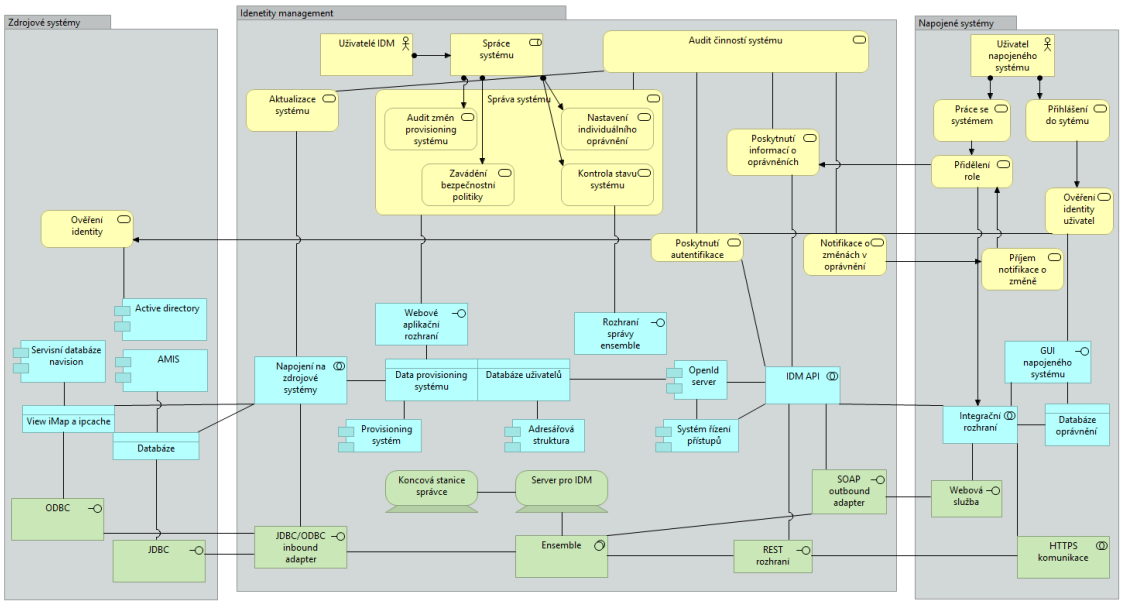
Veškerá komunikace s napojenými systémy musí probíhat pomocí zabezpečeného protokolu HTTPS, všechny činnosti v rámci systému musí být evidovány po dobu minimálně 7 dni.

4 Návrh řešení

V rámci této kapitoly je popsána architektura systému nejprve jako celek a následně specificky pro jednotlivé části, tak jak je využívá jazyk ArchiMate.

4.1 Architektura systému

V rámci této kapitoly je pomocí modelovacího jazyka Archi definována systémová architektura. Ta se skládá z 3 vrstev, mezi které patří business vrstva (v obrázku znázorněna žlutou barvou) sloužící pro popis systému z hlediska business procesů a jejich vlastníků. Následuje aplikační vrstva v rámci, které jsou popsány 3 hlavní pilíře systému a audit. Na závěr této kapitoly je popsána technologická vrstva týkající se datové struktury, napojení na zdrojové systémy a popisu rozhraní.



Obr. 13: Architektura systému [vlastní zpracování]

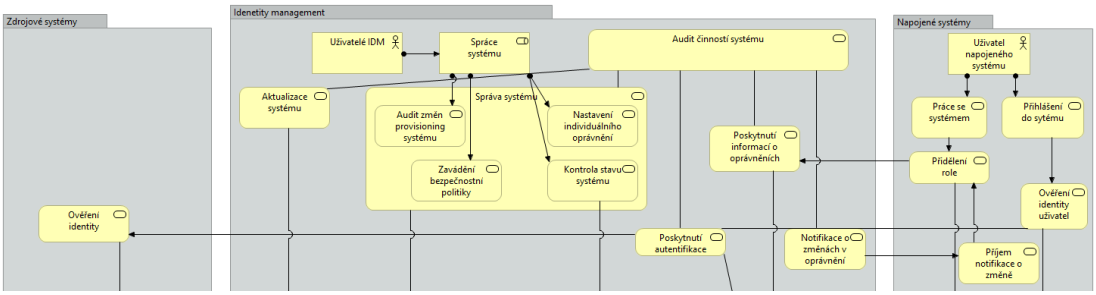
4.2 Business vrstva systému

V rámci business vrstvy jsou popsány základní business služby systému pro jeho plnění, správu, a komunikaci s napojenými systémy.

V rámci systému IDM je hlavním aktérem správce systému, který vykonává veškeré neautomatizované činnosti týkající se správy. Jako je audit změn, zavádění bezpečnostní politiky, nastavení individuálního oprávnění a kontrola systému.

Dále jsou automatizovány činnosti aktualizace systému, logování změn a komunikačních toků, poskytování informacích o oprávněních, poskytování autentifikace vůči vlastní adresářové struktuře nebo Active directory a notifikování o změnách.

V rámci napojených systémů spouští uživatel svým přihlášením proces ověření identity uživatele, který využívá autentifikační služby IDM. V rámci své práce pracovní náplně v daném systému potřebuje oprávnění odpovídající jeho roli v systému, k čemuž využívá autorizační služby IDM. Napojený systém může v případě potřeby přijímat notifikace o změnách v oprávněních a následně si svoji interní strukturu oprávnění aktualizovat.

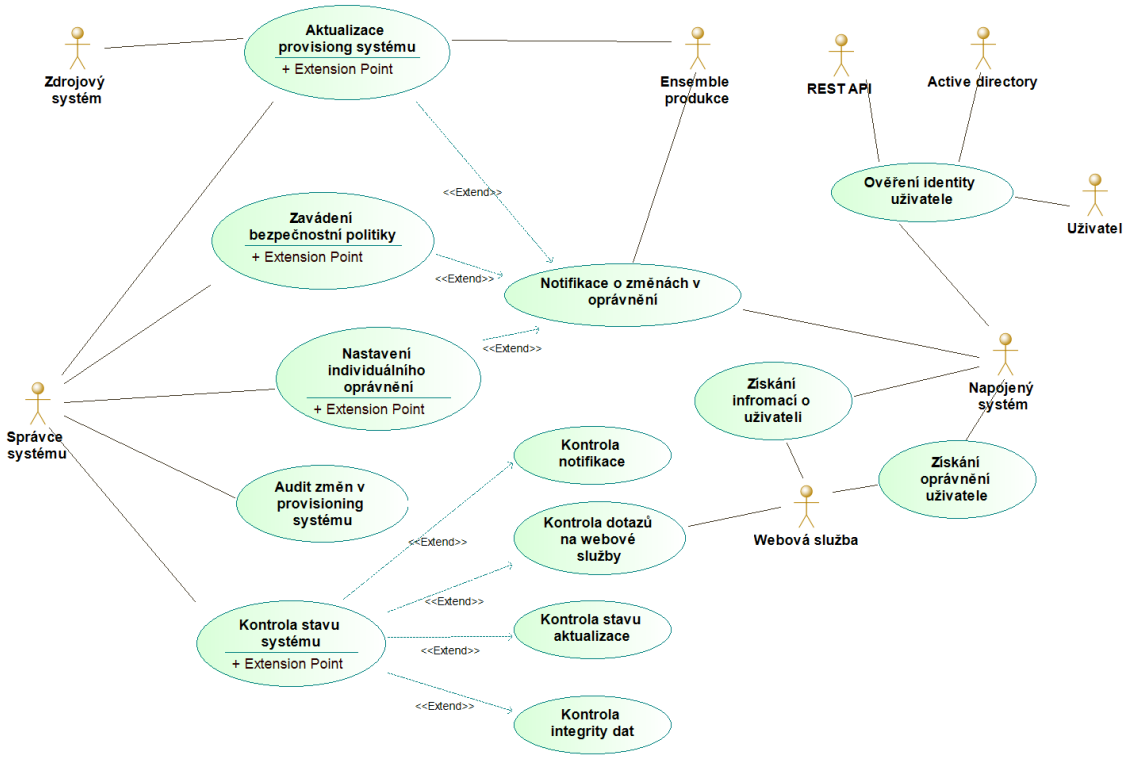


Obr. 14: Business vrstva [vlastní zpracování]

4.2.1 Případy užití

Pro bližší funkční specifikaci je využito případů užití dle standardu UML.

Případ užití popisuje hlavní způsoby využití systému, následně je ke každému případu užití sepsán základní popis pro dané užití dle standardu UML.



Obr. 15: Případy užití [vlastní zpracování]

Tab. 4: Případ užití synchronizace provisioning systému [vlastní zpracování]

Název	Synchronizace provisioning systému		
Popis	Ensemble produkce v pravidelných intervalech spouští synchronizaci se zdrojovými systémy, aktualizuje svoji strukturu a notifikuje o případných změnách		
Primární aktéři	• Ensemble produkce • Provisioning systém • Správce systému		
Sekundární aktéři	• Zdrojové systémy • Napojené systémy		
Vstupní podmínky	• Existuje funkční napojení na zdrojové systémy. • Existuje funkční spojení s napojenými systémy.		
Výstupní podmínky	Struktura provisioning systému je aktualizována bez chyby		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Ensemble produkce	V předem definovaném čase dle rozvrhu spouští business služba v rámci ensemble proces synchronizace.
	2.	Provisioning systém	Replikuje data ze zdrojových systému do struktury globálu pro zpracování, následně provede aktualizaci celé databáze a poskytne seznam osobních čísel pro notifikace
	3.	Provisioning systém	Notifikuje o změnách oprávnění jednotlivých uživatelů
Alt. toky	2 a	Provisioning systém	V rámci procesu aktualizace dojde k odhalení nesrovnalosti ve zdrojových datech provisioning systém odesílá informaci do ensemble produkce a notifikační mail správci systému.
Chybová hlášení	**Číslo**	**Znění**	
	1	-	

Tab. 5: Případ užití zavádění bezpečnostní politiky [vlastní zpracování]

<table>
<tr><td>Název</td><td colspan="3">Zavádění bezpečnostní politiky</td></tr>
<tr><td>Popis</td><td colspan="3">Správce systému pomocí webového rozhraní provisioning systému zavádí bezpečnostní politiku organizace</td></tr>
<tr><td>Primární aktéři</td><td colspan="3">• Provisioning systém
• Správce systému</td></tr>
<tr><td>Sekundární aktéři</td><td colspan="3">• Ensemble produkce
• Napojené systémy</td></tr>
<tr><td>Vstupní podmínky</td><td colspan="3">• Správce oprávnění má zadání bezpečnostní politiky slučitelné s možnostmi nastavení systému</td></tr>
<tr><td>Výstupní podmínky</td><td colspan="3">• Struktura provisioning systému je aktualizována bez chyby</td></tr>
<tr><td>Scénář</td><td>Číslo</td><td>Aktér</td><td>Akce</td></tr>
<tr><td></td><td>1.</td><td>Správce systému</td><td>Pomocí webového rozhraní zavádí a nastavuje typová pracovní místa do systému</td></tr>
<tr><td></td><td>2.</td><td>Správce systému</td><td>Nastavuje pravidla pro přiřazování typových pracovních míst pro jejich automatické přidání na pracovní místa.</td></tr>
<tr><td></td><td>3.</td><td>Provisioning systém</td><td>Notifikuje o změnách oprávnění jednotlivých uživatelů</td></tr>
<tr><td>Alt. toky</td><td>-</td><td>-</td><td></td></tr>
<tr><td>Chybová hlášení</td><td>Číslo</td><td colspan="2">Znění</td></tr>
<tr><td></td><td>1</td><td colspan="2">-</td></tr>
</table>

Tab. 6: Případ užití nastavení individuálního oprávnění [vlastní zpracování]

Název	Nastavení individuálního oprávnění		
Popis	Správce systému pomocí webového rozhraní provisioning systému nastavuje individuální oprávnění pro daného uživatele		
Primární aktéři	• Provisioning systém • Správce systému		
Sekundární aktéři	• Ensemble produkce • Napojené systémy		
Vstupní podmínky	• Správce oprávnění má specifikaci pro nastavení individuálního oprávnění pro uživatele		
Výstupní podmínky	• Struktura provisioning systému je aktualizována bez chyby		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Správce systému	Pomocí webového rozhraní nastavuje na pracovním místě (přidáním rolí, zakázáním rolí z TPM, nastavením speciálních rolí) specifika týkající se pracovní pozice daného uživatele
	2.	Správce systému	Pomocí webového rozhraní nastavuje na jednotlivých pracovních poměrech uživatele (přidáním nebo zakázáním rolí a kompetencí) individuální oprávnění daného uživatele.
	3.	Provisioning systém	Notifikuje o změnách oprávnění jednotlivých uživatelů
Alt. toky	-	-	
Chybová hlášení	**Číslo**	**Znění**	
	1	-	

Tab. 7: Případ užití notifikace o změnách oprávnění [vlastní zpracování]

Název	Notifikace o změnách oprávnění		
Popis	Provisioning systém odesílá do ensemble produkce změny na rolích, typových pracovních místech, pracovních místech a pracovních poměrech uživatele. Ensemble produkce notifikuje napojené systémy o změnách v oprávněních uživatelů.		
Primární aktéři	• Provisioning systém • Ensemble produkce		
Sekundární aktéři	• Napojené systémy		
Vstupní podmínky	• V odpovídajícím namespace je spuštěna ensemble produkce		
Výstupní podmínky	• Napojené systémy přijmou notifikaci bez chyby		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Provisioning systém	Odesílá informace o změnách na rolích, typových pracovních místech, pracovních místech a pracovních poměrech uživatele v podobě ID daného subjektu
	2.	Ensemble produkce	Využívá business procesu „PropagateAccessRights“ k propagování změn k odpovídajícím uživatelům, který poskytuje seznam osobních čísel pro notifikaci
	3.	Ensemble produkce	Využívá odpovídajících operací pro napojené systémy k notifikaci o změnách.
Alt. toky	-	-	
Chybová hlášení	**Číslo**	**Znění**	
	1	-	

Tab. 8: Případ užití ověření identity uživatele [vlastní zpracování]

<table>
<tr><td>Název</td><td colspan="3">Ověření identity uživatele</td></tr>
<tr><td>Popis</td><td colspan="3">Uživatel se v rozhraní napojeného systému autentizuje vůči autentifikačnímu serveru, ten komunikuje s adresářovou strukturou IDM (nebo zavedeného Active directory) pro ověření identity uživatele a poskytuje uživateli token s předem danou platností.</td></tr>
<tr><td>Primární aktéři</td><td colspan="3">• Uživatel
• Napojená aplikace
• Autentifikační server</td></tr>
<tr><td>Sekundární aktéři</td><td colspan="3">• Active directory</td></tr>
<tr><td>Vstupní podmínky</td><td colspan="3">• Uživatel má funkční rozhraní využívající REST služby pro autentifikaci</td></tr>
<tr><td>Výstupní podmínky</td><td colspan="3">• Napojený systém dokáže zpracovat token jako výstup autentizace</td></tr>
<tr><td>Scénář</td><td>Číslo</td><td>Aktér</td><td>Akce</td></tr>
<tr><td></td><td>1.</td><td>Uživatel</td><td>Pomocí rozhraní napojeného systému zadává své přihlašovací údaje</td></tr>
<tr><td></td><td>2.</td><td>Napojený systém</td><td>Odesílá požadavek s přihlašovacími údaji na REST rozhraní autentifikačního serveru</td></tr>
<tr><td></td><td>3.</td><td>Autentifikační server</td><td>Ověřuje přihlašovací údaje proti adresářové struktuře</td></tr>
<tr><td></td><td>4.</td><td>Autentifikační server</td><td>Potvrzuje správnost přihlášení a poskytuje uživateli token s předem danou dobou platnosti pro další prokázání v rámci sezení</td></tr>
<tr><td>Alt. toky</td><td>3a</td><td>Autentifikační server</td><td>Ověřuje přihlašovací údaje proti Active directory.</td></tr>
<tr><td>Chybová hlášení</td><td>Číslo</td><td colspan="2">Znění</td></tr>
<tr><td></td><td>1</td><td colspan="2">Uživatelské jméno nebo heslo nejsou správně</td></tr>
</table>

Tab. 9: Případ užití získání přístupových práv uživatele [vlastní zpracování]

Název	Získání přístupových práv uživatele		
Popis	Po autentizaci uživatele jsou napojeným systémem získány informace o oprávněních		
Primární aktéři	• Uživatel • Rozhraní webové služby • Napojený systém • Ensemble produkce		
Sekundární aktéři	-		
Vstupní podmínky	• Uživatel má platný token pro autentizaci • Napojený systém má funkční napojení na webovou službu		
Výstupní podmínky	• Napojený systém dokáže zpracovat výstup webové služby a nastavit odpovídající oprávnění		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Uživatel	Úspěšně se přihlásí do napojeného systému
	2.	Napojený systém	Volá službu GetRoles pro získání informací o oprávněních uživatele pro daný systém
	3.	Webová služba	Poskytuje odpověď ve formě platných rolí a kompetencí uživatele
	4	Napojený systém	Zpracovává odpověď webové služby a nastavuje uživateli odpovídající role v systému
Alt. toky	1a	Ensemble produkce	Notifikuje o změnách uživatele v momentě jejich pořízení do systému
Chybová hlášení	**Číslo**	**Znění**	
	1		

Tab. 10: Případ užití získání informací o uživateli [vlastní zpracování]

<table>
<tr><td>Název</td><td colspan="3">Získání informací o uživateli</td></tr>
<tr><td>Popis</td><td colspan="3">Po autentizaci uživatele jsou napojeným systémem získány informace o oprávněních</td></tr>
<tr><td>Primární aktéři</td><td colspan="3">• Uživatel
• Rozhraní webové služby
• Napojený systém
• Ensemble produkce</td></tr>
<tr><td>Sekundární aktéři</td><td colspan="3">-</td></tr>
<tr><td>Vstupní podmínky</td><td colspan="3">• Uživatel má platný token pro autentizaci
• Napojený systém má funkční napojení na webovou službu</td></tr>
<tr><td>Výstupní podmínky</td><td colspan="3">• Napojený systém dokáže zpracovat výstup webové služby a nastavit odpovídající oprávnění</td></tr>
<tr><td>Scénář</td><td>Číslo</td><td>Aktér</td><td>Akce</td></tr>
<tr><td></td><td>1.</td><td>Uživatel</td><td>Úspěšně se přihlásí do napojeného systému</td></tr>
<tr><td></td><td>2.</td><td>Napojený systém</td><td>Volá službu GetEmployments pro získání informací uživateli, jeho pracovních poměrech, zařazení hierarchii a jeho oprávněních pro daný systém</td></tr>
<tr><td></td><td>3.</td><td>Webová služba</td><td>Poskytuje odpověď ve formě platných rolí a kompetencí uživatele</td></tr>
<tr><td></td><td>4</td><td>Napojený systém</td><td>Zpracovává odpověď webové služby a nastavuje uživateli odpovídající role v systému</td></tr>
<tr><td>Alt. toky</td><td>1a</td><td>Ensemble produkce</td><td>Notifikuje o změnách uživatele v momentě jejich pořízení do systému</td></tr>
<tr><td>Chybová hlášení</td><td>Číslo</td><td colspan="2">Znění</td></tr>
<tr><td></td><td>1</td><td colspan="2"></td></tr>
</table>

Tab. 11: Případ užití audit změn v provisioning systému [vlastní zpracování]

Název	Audit změn v provisioning systému		
Popis	Správce systému prostřednictvím webového rozhraní systému kontroluje současná oprávnění a ve strukturovaném logu dohledává původ změn v systému		
Primární aktéři	• Správce systému		
Sekundární aktéři	-		
Vstupní podmínky	• Systém logoval změnu oprávnění		
Výstupní podmínky	•		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Správce systému	Po přihlášení do webového rozhraní provisioning systému vyhledá uživatele
	2.	Správce systému	V logu pro uživatele vyhledá původ změny, kterou zkoumá.
	3.	Správce systému	Zobrazí log odpovídající původu zkoumaného stavu s podrobnými informacemi o změně
Alt. toky			
Chybová hlášení	**Číslo**	**Znění**	
	1		

Tab. 12: Případ užití kontrola stavu systému [vlastní zpracování]

Název	Kontrola stavu systému		
Popis	Správce systému přistupuje do příslušného rozhraní, kde kontroluje notifikace, komunikaci s napojenými systémy, stav synchronizace a integritu dat.		
Primární aktéři	• Správce systému		
Sekundární aktéři			
Vstupní podmínky	• Systém logoval změnu oprávnění		
Výstupní podmínky	•		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Správce systému	Zobrazí rozhraní správy systému
	2.	Správce systému	Získá podrobné informace o: notifikacích, komunikaci s napojenými systémy, stavu aktualizace a integritě dat.
	3	Správce systému	Neshledá žádnou nesrovnalost v chodu systému.
Alt. toky	3a	Správce systému	Shledá nesrovnalosti, informuje o ní příslušné odpovědné osoby a sjedná příslušnou nápravu
Chybová hlášení	**Číslo**	**Znění**	
	1		

Tab. 13: Případ užití kontrola notifikace [vlastní zpracování]

Název	Kontrola notifikace		
Popis	Správce systému přistupuje do rozhraní ensemble produkce, kde kontroluje notifikace a v případě nesrovnalosti opakuje odeslání a tím vyžádá synchronizaci s napojenými systémy.		
Primární aktéři	• Správce systému		
Sekundární aktéři	• Napojené systémy • Ensemble produkce		
Vstupní podmínky	• Systém logoval změnu oprávnění		
Výstupní podmínky	•		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Správce systému	V rozhraní ensemble produkce kontroluje stav odchozích notifikací za posledních 7 dní.
	2.	Správce systému	Nachází nesrovnalosti v průchodu notifikací do napojených systému
	3.	Správce systému	Opakuje odeslání notifikace a čeká na odpověď daného systému pro kontrolu obdržení notifikace
	4.	Správce systému	Informuje odpovědnou osobu o stavu a eviduje chybu.
Alt. toky	2a	Správce systému	Nenachází nesrovnalosti v průchodu notifikací.
Chybová hlášení	**Číslo**	**Znění**	
	1		

Tab. 14: Případ užití kontrola dotazů na webové služby [vlastní zpracování]

Název	Kontrola dotazů na webové služby		
Popis	Správce systému přistupuje rozhraní ensemble produkce, kde kontroluje komunikaci s napojenými systémy a v případě chyby napojení využívá nápravné mechanismy pro obnovení napojení		
Primární aktéři	• Správce systému		
Sekundární aktéři	• Ensemble produkce • Napojený systém		
Vstupní podmínky	• Systém logoval změnu oprávnění		
Výstupní podmínky	•		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Správce systému	V rozhraní ensemble produkce kontroluje stav komunikace s napojenými systém za posledních 7 dní.
	2.	Správce systému	Nachází nesrovnalosti v komunikaci s napojenými systému
	3.	Správce systému	Kontraktuje odpovědného správce napojeného systému pro zjištění příčiny chyby v komunikaci a obnovení spojení v komunikaci.
	4.	Správce systému	Eviduje chybu s odpovídající příčinou a v případě potřeby kontaktuje dodavatele systému pro opravu chyby.
Alt. toky	2a	Správce systému	Nenachází nesrovnalosti v komunikaci s napojenými systémy.
Chybová hlášení	**Číslo**	**Znění**	
	1		

Tab. 15: Případ užití kontrola stavu synchronizace [vlastní zpracování]

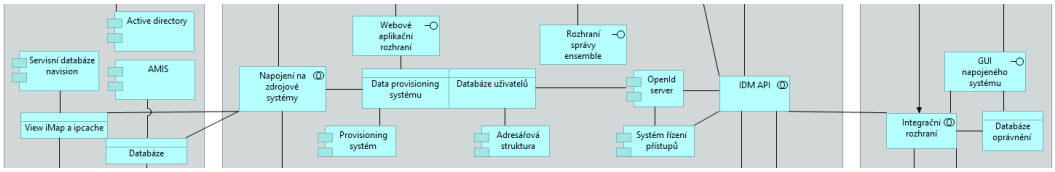
Název	Kontrola stavu synchronizace		
Popis	Správce systému přistupuje rozhraní správy aktualizace a integrity dat, kde kontroluje stav aktualizace a případné nesrovnalosti v aktualizaci ze zdrojových systémů		
Primární aktéři	• Správce systému		
Sekundární aktéři	• Ensemble produkce • Zdrojový systém		
Vstupní podmínky	• Systém začal aktualizaci ze zdrojového systému		
Výstupní podmínky	• Provisioning systém aktualizovat databázi uživatelů a databázi provisioning systému		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Správce systému	V rozhraní pro správu aktualizace zobrazí průběh poslední aktualizace.
	2.	Správce systému	Kontroluje stav jednotlivých částí aktualizace.
	3.	Správce systému	Nachází nesrovnalosti v průchodu aktualizace a získá podrobnější informace o původu chyby.
	4.	Správce systému	Kontraktuje odpovědného správce zdrojového systému pro zajištění opravy chyby ve zdrojovém systému a opakuje aktualizaci
	5	Správce systému	Eviduje chybu s odpovídající příčinou a v případě potřeby kontaktuje dodavatele systému pro opravu chyby.
Alt. toky	3a	Správce systému	Nenachází nesrovnalosti ve stavu aktualizace.
Chybová hlášení	**Číslo**	**Znění**	
	1		

Tab. 16: Případ užití kontrola integrity dat [vlastní zpracování]

Název	Kontrola integrity dat		
Popis	Správce systému přistupuje rozhraní pro aktualizaci a integritu dat, kde stav integrity dat a řeší případné nesrovnalosti, vyhledáním jejich původu a následnou opravou		
Primární aktéři	• Správce systému		
Sekundární aktéři	• Ensemble produkce • Napojený systém		
Vstupní podmínky	•		
Výstupní podmínky	• Integrita dat systému je v pořádku		
Scénář	**Číslo**	**Aktér**	**Akce**
	1.	Správce systému	V rozhraní pro správu integrity dat zobrazí momentální stav integrity dat.
	2.	Správce systému	Nachází nesrovnalosti v integritě (náladové středisko použité na pracovním poměru není zavedeno do číselníku nákladových středisek)
	3.	Správce systému	Kontraktuje odpovědného správce napojeného systému pro zjištění příčiny chyby v integritě a napravení situace.
	4.	Správce systému	Eviduje chybu s odpovídající příčinou a v případě potřeby kontaktuje dodavatele systému pro opravu chyby.
Alt. toky	2a	Správce systému	Nenachází nesrovnalosti v integritě systému.
Chybová hlášení	**Číslo**	**Znění**	
	1		

4.3 Aplikační vrstva

V rámci této kapitoly je popsána aplikační vrstva systému. Vlastní systém se skládá ze tří hlavních částí a to z Provisioning systému, adresářové struktury a tzv. Access Managera. Každá z hlavních částí bude popsána níže



Obr. 16: Aplikační vrstva [vlastní zpracování]

4.3.1 Provisioning systém

Provisioning systém se stará v první řadě o napojení na zdrojové systémy, kterými jsou Navision pro ekonomická a personální data a AMIS pro data medicínská týkající se především organizační struktury.

Napojení na zdrojové systémy

Pro napojení na systém Navision je možné využít SQL view, které neumožňuje spojení přímo s vlastní databází systému, ale se servisní databází, která je synchronizována s vlastní databází systému každý den.

V návaznosti na tuto synchronizaci se servisní databází je možné napojit synchronizační proces pro personální a ekonomická data

Napojení personálního systému

Personální systém poskytuje data o zaměstnancích, jejich pracovních poměrech, které dále obsahují pracovní pozice, které zastávají, jejich časovou platnost, definici pracovních činností pomocí jmenovky a povolání a hodnoty úvazku. Všechny tyto data

jsou před začátkem synchronizace replikována do databáze Ensemble pro umožnění rychlejšího zpracování.

Pro unikátní identifikátor pracovního poměru zaměstnance je možné využít složeného primárního klíče **Osobní číslo** a **číslo poměru** (Employee_No a Employment_No). Je možné, aby měl zaměstnanec více odpovídajících záznamů, proto je třeba brát v potaz parametr CurrentFlag, který musí být 1.

Tyto platné poměry mohou být aktivní nebo neaktivní, k určení je nutné brát v potaz položky začátku a konce pracovního poměru a speciální položku identifikující evidenční stav (Evidentary_Count), Jejíž vyplněná hodnota identifikuje například nástup na mateřskou dovolenou, do vězení a další.

Napojení systému plánování podnikových zdrojů

Obdobně jako u personálního systému je pro systém plánování podnikových zdrojů replikována databáze, která obsahuje strukturu nákladových středisek v hierarchii o 3 úrovních

1) Organizace (FN Brno)
2) Klinika
3) Nákladové středisko kliniky

Pro identifikaci platného nákladového střediska je využito položky označující datum ukončení platnosti, Pokud je prázdná nebo vyšší než daný den je možné brát středisko jako platné.

Dále je nutné identifikovat kliniku. To je možné pomocí nadřazeného nákladového střediska, které má klinika sama na sebe a účtování, které je na klinice zablokováno.

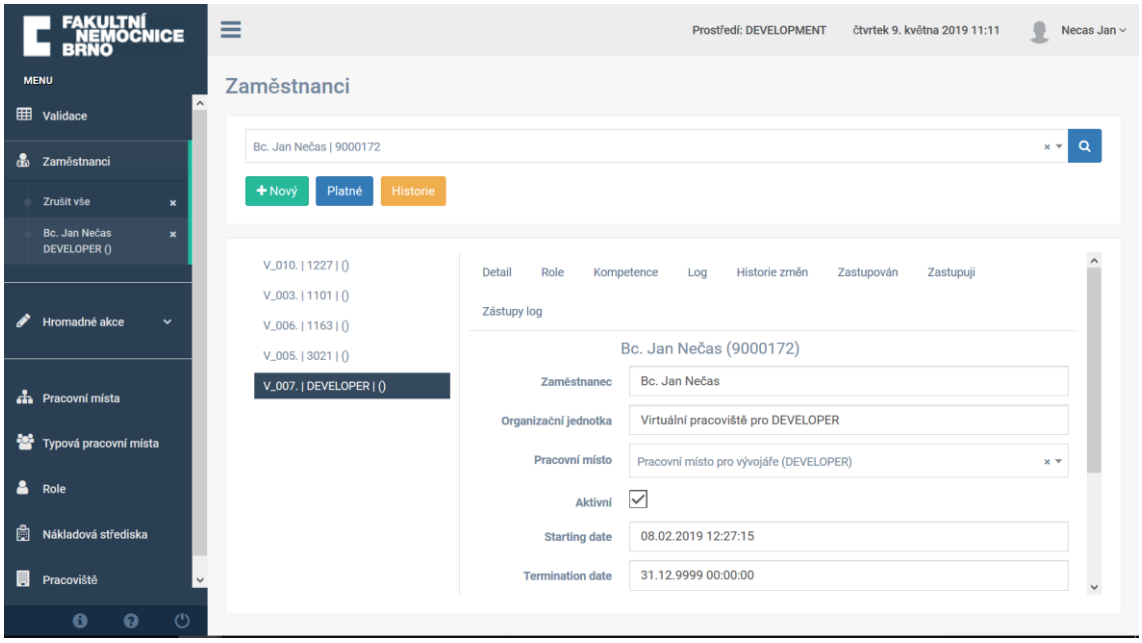
Napojení klinického informačního systému

Klinický informační systém AMIS*H je nepojen pomocí ODBC konektoru přímo do jeho zdrojové databáze. Jsou z něj čerpána data o medicínských pracovištích a to především jejich odbornostech, identifikačních číslech pracoviště a hierarchiích.

Uživatelské rozhraní

Pro uživatelské rozhraní aplikace pro správu provisioning systému je využito moderního vývojového frameworku Angular.

Pro rychlou orientaci v systému je menu stále dostupné v levé části obrazovky s možností jeho schování. Obsahuje možnost přecházet mezi hlavními částmi aplikace pro správu oprávnění na různých úrovních a uchovává rozpracovanou práci v systému. Pod menu je ukotvený řádek obsahující informace o systému, přístup do dokumentace a tlačítko pro odhlášení. V horní hlavičce je pro uživatele jednoduchá identifikace pro aktuální prostředí kde se nachází. Ať už je vývojové, testovací nebo produkční.

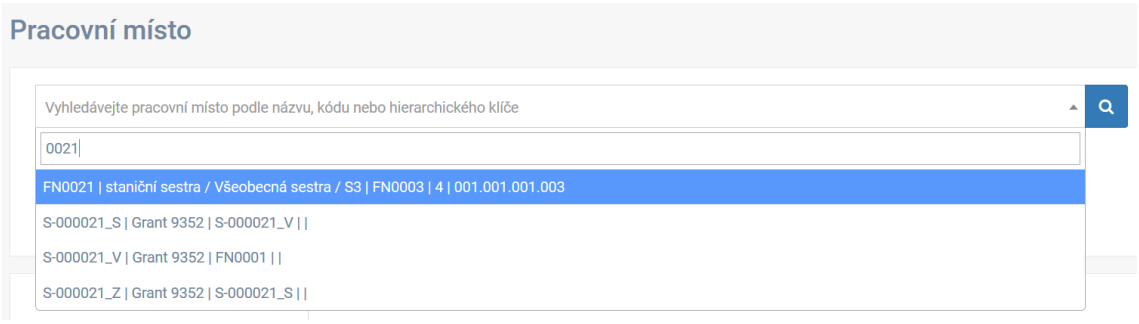


Obr. 17: Uživatelské rozhraní provisioning systému [vlastní zpracování]

Vlastní práce s aplikací probíhá pomocí 3 základních nástrojů, které jsou společné pro všechny části aplikace. Takto je umožněno uživateli jednotně přistupovat k problematice oprávnění napříč celým systémem a využití intuice při práci s aplikací.

Vyhledání v aplikaci

Probíhá pomocí vyhledávacího selectboxu. Ten obsahuje informace o možnostech vyhledávání a v případě zadání prvních dvou znaků nabízí relevantní možnosti. Při najetí kurzorem myši zvýrazní daný řádek



Obr. 18: Vyhledávání v aplikaci [vlastní zpracování]

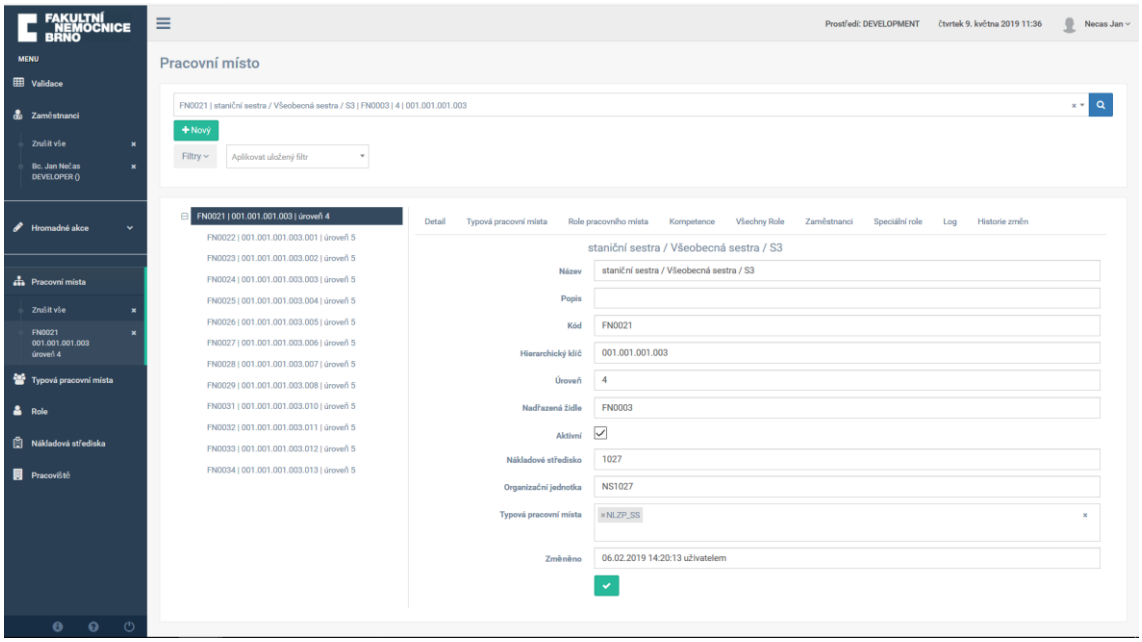
Výběr ze seznamu

Jelikož při vyhledání může nastat situace, více relevantních informací je v systémů další klíčovou komponentou výběr ze seznamu. Ten může obsahovat třeba všechny pracovní poměry daného zaměstnance jak je tomu vidět v obrázku 17. Další z využití seznamu je pro zobrazení hierarchie, která může mít více úrovní. Tyto úrovně je možné otevírat a zavírat pomocí ovládacích prvků seznamu.

Obr. 19: Hierarchický seznam [vlastní zpracování]

Detailní zobrazení

Po úspěšném výběru je pro uživatele zobrazen detail jako první z více záložek pro danou část aplikace. Ty mohou pro různé části být odlišné, ale záložky detailu a logu jsou pro všechny stejné. Záložky slouží pro zobrazení dle umístění pro správu typových pracovních míst, rolí, kompetencí, nebo mohou zobrazovat využití pro roli, typové pracovní místo a pracovní místo.



Obr. 20: Záložky pracovního místa [vlastní zpracování]

4.3.2 Adresářová struktura

Vlastní adresářová struktura je uchovávána v podobě objektově popsaného globálu, tato technologie umožňuje jak rychlé čtení, tak jednoduchou replikaci pro zvýšení dostupnosti a bezpečnosti dat.

Struktura adresářové struktury je následující:

Tab. 17: Atributy adresářové struktury [vlastní zpracování]

Název	Typ	Popis
ADAccounet	String	účet do Active directoty (doména\osobníčíslo)
AcademicalDegree	String	Titul za jménem
Certificate	Serializovaná třída	Informace o certifikátu
DateModified	Time Stamp	Datum poslední změny
EmployeeNo	String	Osobní číslo pracovníka
FirstName	String	Křestní jméno
Gender	String	Pohlaví
LastName	String	Příjmení
ModifiedBy	String	Poslední změna provedena uživatelem (osobní číslo, systém, který změnil).
Name	String	Celé jméno i s tituly před a za jménem
Primary Contact	Serializovaná třída	Kontaktní informace
RootCostCenter	String	Kmenové nákladové středisko pro pracovníka z pracoviště, kde má největší pracovní poměr.
Signature	String	Podpis
Tile	String	Titul před jménem

4.3.3 Systém řízení přístupů

Základními úkoly systému řízení přístupů jsou možnosti poskytování autentifikace a autorizace. Jako rozšíření je v rámci tohoto systému definována i možnost notifikace napojeným systémům o změnách.

Autentifikace

Pro problematiku autentifikace je v tomto sytému využito open source projektu MITREid Connect, který pracuje se standardem OAUTH 2 a UMA. V rámci systému ensemble je možné zprostředkovat delegovanou autentifikaci například pomocí standardu OAUTH 2

V tomto návrhu umožňuje Open Id server napojení na nemocniční Active Directory, Tudíž se uživatelé mohou připojovat pomocí jejich stávajícího jména a hesla. Výhodou je, že tímto zaniká nutnost přenášení hesla do databáze Ensemble a tím zvýšení hrozby úniku těchto dat.

Autorizace

Autorizace v systému je zabezpečovaná pomocí Webové služby obsahující 2 základní způsoby ověření přístupových práv *Metody GetRoles a GetEmployments.* Rozhraní webové služby je popsáno ve vlastní kapitole níže.

Autorizace je možné poskytnout na základě architektury rolí (RBAC) a kompetencí. Záleží na každém napojovaném systému, jak jemně si oprávnění chce řídit. Může být řešen přístupem do systému jako celku, nebo řízením přístupu pro menší přesněji definované celky.

Vlastní datová struktura obsahuje dynamicky generované kompetence k jednotlivým rolím, díky nim je možné přiřazovat uživatelům pouze role s kompetencí provádět změny

na nákladovém středisku nebo klinice, konkrétní hodnoty daného nákladového střediska, nebo kliniky jsou individuálně získány z informací v pracovním poměru.

Pro zrychlení odezvy dotazů na oprávnění uživatele je vytvořena struktura **User**, která obsahuje hlavní výstup pro informace uživatele. Do této struktury se při každé aktualizaci v provisioning systému odesílá notifikace o změně, v návaznosti na tuto notifikaci se struktura aktualizuje pomocí dotazu na práva, která jsou následně dynamicky vypočítávána.

Systém samotného poskytnutí autorizace může probíhat ve dvou typech napojení a to *aktivním* a *pasivním*. V rámci aktivního napojení se systém dotazuje při přihlášení uživatele na jeho aktuální oprávnění a dle nich mu povoluje, nebo zakazuje vykonávat jednotlivé činnosti. Jelikož ne každý systém je schopen takto vyčlenit oprávnění uživatele ze svého jádra, je navržen pasivní typ napojení pracující s notifikací popsanou níže.

Notifikace

Jako rozšíření standartního přístupu ke správě přístupů je navržen systém notifikace o změnách na uživateli. Z důvodu dynamického generování oprávnění je při změně definice oprávnění role nutné generovat všechny navazující struktury až po uživatele oprávněné danou roli zastávat. Následně pomocí napojení na rozhraní připojených systému probíhá vlastní notifikace o změnách v oprávnění uživatele.

Systém těchto notifikací je realizován v rámci Ensemble produkce, což zaručuje přehled notifikovaných změn, a případné logování chyb v rámci celého procesu notifikace. V neposlední řadě tato realizace umožňuje od napojeného systému získat zpětnou vazbu na obdržení notifikace, která může indikovat chybu v napojeném systému správci před tím, než omezí uživatele ve výkonu práce.

Vlastní notifikace obsahuje pouze osobní číslo uživatele. V návaznosti na obdržení notifikace se napojený systém dotáže na oprávnění uživatele standartní cestou pomocí webové služby popsané v části autorizace.

4.3.4 Audit systému

V rámci všech tří hlavních částí provisioning systému, adresářové struktury a systému řízení přístupů jsou vedeny logy o jednotlivých činnostech do níže popsaného detailu.

Audit provisioning systému

Pro audit provisioning systému jsou využity aplikační logy zaznamenávající činnosti identity management a automatických aktualizací. Zmíněné logy zaznamenávají následující informace o změnách:

- Autora změny: osobní číslo uživatele nebo název automatické činnosti
- Čas provedení změny: případně její propsání v rámci struktury systému
- Typ změny: může jít o inicializační log, změnu oprávnění a další
- Zdroj změny: v případě propsání oprávnění z role bude uvedeno „ROLE“
- Název změny: – v případě propsání z role bude uveden kód role

Audit adresářové struktury

Pro adresářovou strukturu uchovávanou jako, persistentní objekt, je využit serializovaný objekt s názvem *BaseInfo* ten ukládá následující informace:

- Name – název daného záznamu,
- Description – popis,
- Use – příznak zda má být záznam používán,
- Active – příznak zda je záznam aktivní,
- ModifiedBy – osobní číslo, (nebo identifikace systému) autora poslední změny,
- ModifiedAt – čas poslední změny.

Audit systému řízení přístupů

Audit pro systém řízení přístupů je rozdělen do 3 částí stejně jako systém vlastní. Pro audit *autentifikace* jsou využity logovací mechanismy využitého opensource softwaru evidující poskytnuté tokeny jednotlivým identitám s dobou jejich platnosti.

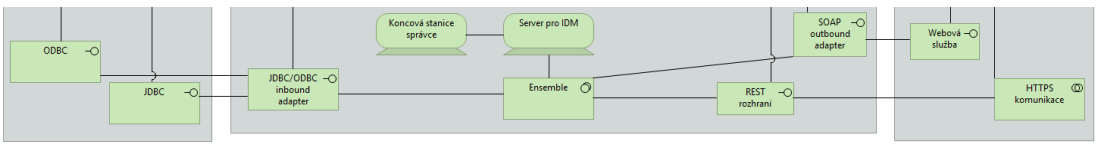
Pro audit *autorizace* jsou evidovány dotazy na oprávnění jednotlivých identit, dotazy jsou evidovány v následujícím formátu:

- Dotazující uživatel – systém nebo uživatel dotazující se webové služby,
- Požadavek – parametry požadavku na data,
- Odpověď – poskytnutá odpověď systémem,
- Čas dotazu – čas, ve kterém se uživatel nebo systém dotázal,
- Metoda – metoda využitá pro dotaz

Pro audit *notifikací* jsou evidovány odeslané notifikace do každého z napojených systému odděleně. Jsou evidována notifikovaná osobní čísla a odpověď, kterou systém na zaslanou notifikaci poskytl.

4.4 Technologická vrstva

V rámci této kapitoly je popsána technologická vrstva systému, která specifikuje datový model systému, napojení IDM na zdrojové systémy a rozhraní komunikace s napojenými systémy.

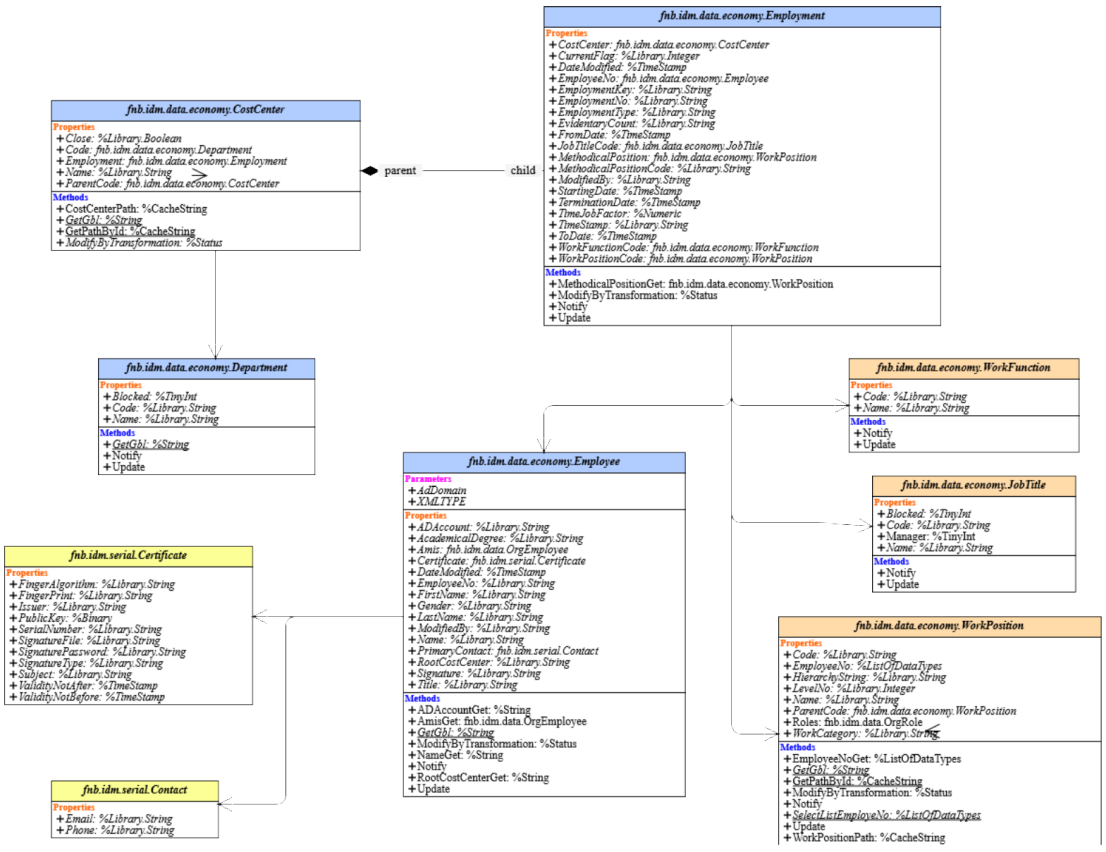


Obr. 21: Technologická vrstva [vlastní zpracování]

4.4.1 Datová struktura

Datová struktura systému je dělena do 2 hlavních částí. První uchovává informace o uživatelích a jejich pracovních poměrech pro řízení životního cyklu identity. Tato struktura je primárně založena na datovém modelu personálního systému.

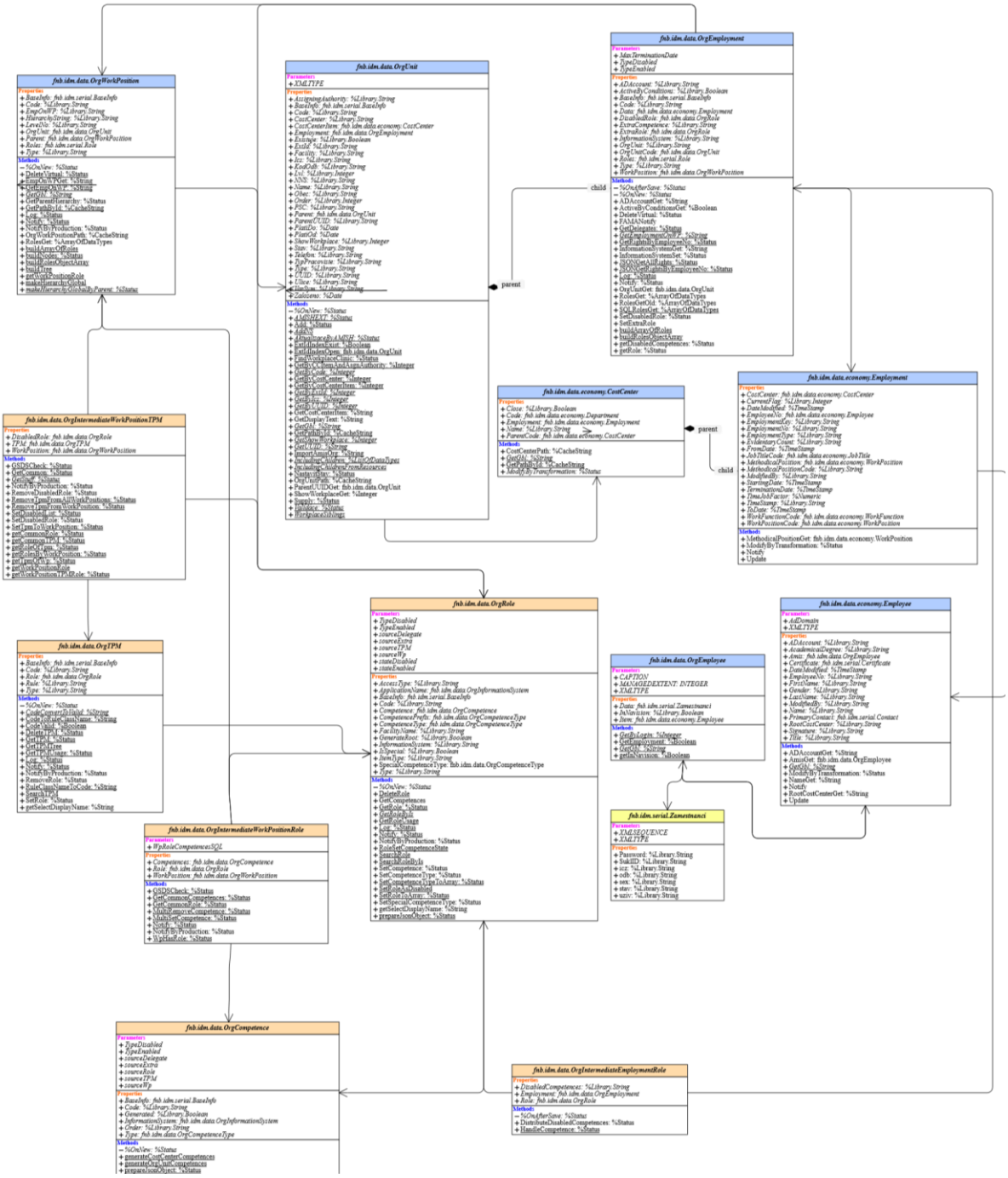
Diagram níže zobrazuje datovou strukturu pro ekonomická data



Obr. 22: Datová struktura ekonomických dat [vlastní zpracování]

Druhá část rozšiřuje informace o pracovních poměrech pro jemnější dělení medicínských systémů, dále umožňuje realizaci funkčních požadavků na správu rolí na úrovni pracovního poměru a typového pracovního místa, aplikačně je pro každé pracovní místo vytvářeno vlastní typové pracovní místo pro realizaci požadavku přidání rolí přímo na pracovní místo.

Schéma datové struktury je podrobněji zobrazeno v přílohách. Na obrázku níže je zobrazena struktura systému bez ekonomické části napojené na pracovní poměr.



Obr. 23: Datová struktura systému [vlastní zpracování]

4.4.2 Technologie klientské aplikace

Pro realizaci aplikace správy IDM slouží webová aplikace využívající poslední verze technologie Angular, která je napojena na aplikační REST API systému Ensemble realizovaném pomocí rozšíření předdefinované třídy *%CSP.Base*.

Pro možnost přesměrování požadavků na serveru bude využito strukturovaného URL volání. V rámci veškeré komunikace týkající se IDM bude využíváno začátku volání klíčové slovo *ORGUNIT*. Pro následné přesměrování bude struktura požadavků odpovídat datové struktuře aplikace.

4.4.3 Napojení na zdrojové systémy

Zdrojové systémy jsou napojeny pomocí SQL gateway využívajícím technologii JDBC/ODBC.

Tab. 18: Struktura informací systému Navision HR [vlastní zpracování]

Databáze	Schéma	Tabulka	Popis
MZSERVIS	Map	iEmployee	Infromace o uživatelích (identitách)
MZSERVIS	Map	iEmployment	Infromace o pracovních poměrech uživatele
MZSERVIS	Map	iWorkPosition	Informace o pracovních pozicích v rámci hierarchie
MZSERVIS	Map	iWorkFunction	Informace o povoláních, slouží jako číselník povolání pro pracovní poměry (například Lékař, Sestra, Vedoucí pracovník atd.)
MZSERVIS	Map	iWorkTitle	Informace o jmenovkách, specifikují v rámci povolání bližší specializaci (například staniční sestra, vrchní sestra atd.)

Dále je ze servisní databáze pro systém plánování podnikových zdrojů čerpány následující informace.

Tab. 19: Struktura informací systému Navision ERP[vlastní zpracování]

Databáze	Schéma	Tabulka	Popis
MZSERVIS	Ipcache	Department	Informace o nákladových střediscích
MZSERVIS	Ipcache	DepartmentPH	Informace o nákladových střediscích, omezeních v účtování, návaznosti na další systémy.

4.4.4 Komunikace s napojenými systémy

Pro komunikaci s napojenými systémy jsou 2 hlavní komunikační toky první pomocí rest rozhraní poskytující autentifikaci identity a druhý realizovaný webovou službou poskytující autorizaci uživatele.

REST rozhraní

Server pomocí REST rozhraní poskytuje autentifikační službu pro aplikace pomocí komunikace přes zabezpečený HTTPS protokol. Níže je uvedený příklad volání metodou POST obsahující parametry v URL pro uživatele a heslo

https://ServerName//api/auth/token?grant_type=password&username=<uživatel>&password=<heslo>

Příklad pro osobní čísla:

- externí pracovníky (9000172) řada začínající 9000000
- interní pracovníky (1416) řada 0 - 99999

Vlastní služba je zabezpečena kombinací jména a hesla, které se zakódované předává v hlavičce v poli Authorizaction

Jako odpověď přijde při úspěšné autentifikaci uživateli v poli „access_token“ vlastní token s danou platností, kterým se může uživatel dále prokazovat.

SOAP rozhraní

V rámci SOAP rozhraní jsou definovány služby poskytující informace o oprávněních uživatele pro daný systém, nebo o celkových informacích o uživateli včetně jeho kontaktních údajů, pracovních poměrů, oprávněních, zařazení v hierarchii.

Služba GetRoles

Vyhledá všechny role zaměstnance podle osobního čísla. Při zaslání requestu lze specifikovat informační systém pomocí elementu: <ApplicationName>

Tab. 20: Požadavek pro GetRoles [vlastní zpracování]

Název	Element	Popis
Osobní číslo	<PersonalId>	Osobní číslo zaměstnance . **Povinná položka**
Informační systém	<ApplicationName>	Informační systém pro který bude služba vracet role **Výchozí hodnota je Vše**
Aktivní poměr	<CurrentFlag>	Logická hodnota pro zobrazování práv nad aktivními poměry: • 1 aktivní • 0 neaktivní

Při úspěšném volání odpovídá systém odpovědí o následující struktuře:

Tab. 21: Odpověď pro GetRoles [vlastní zpracování]

Název	Element	Popis
Zaměstnanec	<Employee>	obsahuje osobní číslo zaměstnance a počet rolí
Role	<Roles>	Pole obsahující jednotlivé role ve struktuře popsané níže

Tab. 22: Struktura elementu Role [vlastní zpracování]

Název	Element	Popis
Role	<Role>	obsahuje klíč role a počet kompetencí k roli
Informační systém	<ApplicationName>	Informační systém pro který role platí

Kompetence	<Competence>	Včet kompetencí k dané roli s informacemi o:
		• Informační systém
		• Code (kód kompetence)
		  ○ NS - Nákladové středisko
		  ○ UO - Klinika
		  ○ CO - Centrum odpovědnosti
		• Computed (výpočtová)
		• Source (zdroj: Role, Extra)
		• Is Valid (validní kompetence pro systém FAMA)
		• CompetenceType (typ kompetence přebýraný z role)
		• FullCode (TypKompetence + Kód kompetence)

GetEmployments

Vyhledá všechny aktivní úvazky zaměstnance podle osobního čísla. Ke každému úvazku jsou přiděleny i role a kompetence k jednotlivým informačním systémům.

V případě, že služba GetEmployments nevrátí žádná data, daný pracovník nemá žádný aktivní employment, tudíž nemá žádná práva

V případě nastavené zastupitelnosti obsahuje Zastupovaný employment element <Delegate> ten obsahuje, poměr Zastupujícího i s jeho přístupovými právy.

Tab. 23: Požadavek pro GetEmployments [vlastní zpracování]

Název	Element	Popis
Žádající uživatel	<RequestingUser>	Uživatelské jméno přidělené správcem integrační platformy pro komunikaci s webovou službou
Osobní číslo	<PersonalId>	Osobní číslo zaměstnance, pro kterého jsou vyžadována oprávnění
Příznak aktivity	<CurrentFlag>	Příznak pro aktivní pracovní poměry plnit hodnotou 1

Každý aktivní poměr si nese následující informace:

Tab. 24: Odpověď pro GetEmplyments [vlastní zpracování]

Název	Element	Popis
Nákladové středisko	<OrgUnit>	Nákladové středisko na kterém je poměr založen ve zdrojové databázi
Data	<Data>	Informace ze zdrojové databáze Navision HR nese informace o pracovním poměru ve struktuře popsané níže
Pracovní místo (Židle)	<WorkPosition>	pro každou židli jsou zaslány i židle nadřízené v hierarchii až k nejvyšší židli. Židle si dále nese i zaměstnance na židli, element <EmpOnWp>
Role	<Roles>	Pole rolí, které jsou pro daný poměr přidělené. struktura popsána níže
Základní informace	<BaseInfo>	Informace o aktivitě a poslední úpravě
Účet v active directory	<ADAcount>	účet v active directory ve formátu **domény/login**

V rámci odpovědi na pracovní poměry uživatele je obsažen XML projekce pracovního poměru a jeho ekonomické strukury.

Tab. 25: Struktura elementu Data [vlastní zpracování]

Název	Element	Popis
Identifikátor poměru	<EmploymentKey>	obsahuje identifikátor daného poměru v ekonomické struktuře.
Informace o zaměstnanci	<EmployeeNo>	Informace o zaměstnanci ve struktuře popsané níže
Číslo poměru	<EmploymentNo>	Číslo pracovního poměru nabývá hodnot: 1-99 fyzické poměry pro řadu virtuálních poměrů nabývá hodnot V_001-V_999
Jmenovka	<JobTitleCode>	Jmenovka přesněji specifikující pracovní náplň v rámci poměru. Ve struktuře <CODE>, <NAME>
Povolání	<WorkFunctionCode>	Povolání obecně specifikující pracovní náplň daného poměru. Ve struktuře <CODE>, <NAME>
Pracovní místo	<WorkPositionCode>	Pracovní místo specifikuje zařazení pracovního poměru v rámci hierarchie. V následující struktuře: • Code - kód pracovního místa • Name - název pracovního místa • LevelNo - úroveň řízení • ParentCode - vazba na nadřazené pracovní místo.

Součástí odpovědi jsou oprávnění uživatele pro každý z pracovních poměrů. Ve stejné struktuře jako jsou poskytovány službou GetRoles popsány v tabulce 22 výše

GetEmployee

Vyhledává zaměstnance podle osobního čísla (doménový login) nebo uživatelského jména v systému AMIS*H.

Tab. 26: Požadavek pro GetEmployee [vlastní zpracování]

Název	Element	Popis
Osobní číslo	<StringValue>	Osobní číslo zaměstnance, pro kterého jsou vyžadovány přesnější informace

Tab. 27: Odpověď pro GetEmployee [vlastní zpracování]

Název	Element	Popis
Infromace pro medicínské systémy	<Data>	Informace o zaměstnanci pro medicínské systémy v následující pod struktuře elementů: • sex - pohlaví (M/Z) • stav - ukazatel zda má daný pracovník aktivní pracovní poměr (A/X) • uziv - uživatelské jméno do systému AMIS • SuklID - identifikátor lékaře pro Státní ústav pro kontrolu léčiv
Infromace pro ekonomické systémy	<Item>	Informace o zaměstnanci pro ekonomické systémy popsané ve struktuře níže

Tab. 28: Informace o zaměstnanci pro ekonomické systémy [vlastní zpracování]

Název	Element	Popis
Osobní číslo	<EmployeeNo>	Osobní číslo zaměstnance (Primární identifikátor)
Křestní jméno	<FirstName>	Křestní jméno
Příjmení	<LastName>	Příjmení
Akademický titul	<Title>	Akademický titul
Pohlaví	<Gender>	Pohlaví
Certifikát	<Certificate>	Obsahuje informace o sériovém číslo certivikátu • <SerialNumer>

Kontaktní informace	<PrimaryContact>	Obsahuje kontaktní informace daného zaměstnace • <Email> - email • <Phone> - telefonní číslo
Účet v active directory	<ADAcount>	účet v active directory ve formátu **domény/login**
Kmenové nákladové středicko	<RootCostCenter>	Nákladové středisko kde má daný pracovník pracovní poměr s největším úvazkem
Celé jméno	<Name>	Celé jméno a příjmenení s tituly před i za jménem

GetOrgUnit

Umožní vyhledat podrobné informace o pracovišti podle identifikátorů zdrojových systémů nebo unikátního identifikátoru UUID.

Tab. 29: Požadavek pro službu GetOrgUnit [vlastní zpracování]

Název	Element	Popis
Identifikátor pracoviště	<StringValue>	identifikátor lze specifikovat podle: • identifikátoru AMIS*H (serorg) • identifikátoru GUID (UUID) • Kód pracoviště (Code např "B-CHK-A") • IČZ (Identifikační číslo poskytovatele)

Služba poskytuje odpověď s níže specifikovanými informacemi

Tab. 30: Odpověď pro službu GetOrgUnit [vlastní zpracování]

Název	Element	Popis
UUID pracoviště	<UUID>	UUID pracoviště dotazovaného pracoviště
Kód pracoviště	<Code>	Kód dotazovaného pracoviště
Externí ID	<ExtId>	ID daného pracoviště v externím systému pro AMIS*H = Serorg
Název pracoviště	<Name>	Název dotazovaného pracoviště

Nadřazené pracoviště	<Parent>	UUID pracoviště nadřazeného dotazovanému pracoviště
Úroveň pracoviště	<Lvl>	Úroveň pracoviště v hierarchii
Nákladové středisko	<CostCenter>	Nákladové středisko pracoviště ze systému AMIS*H
Nákladové středisko z NAVISION	<CostCenterItem>	Nákladové středisko pracoviště ze systému NAVISION
Typ Pracoviště	<TypPracoviste>	Typ pracoviště: • stan (Lůžkové oddělení) • amb (ambulance) • lab (laboratoř) • tra (transfůzní oddělení) • rtg (rentgen) • pat (patologie) • ope (operační sál) • hem (hematologická laboratoř) • jip (jednotka intenzivní péče) • ext (externí pracoviště)
Nadřazené nákladové středisko	<NNS>	Nadřazené ákladové středisko pracoviště ze systému NAVISION
Stav	<Stav>	Stav pracoviště: • A (aktivní) • X (Neaktivní)
Založeno	<Zalozeno>	Datum založení pracoviště
Platí Od	<PlatiOd>	Datum kdy všešlo pracoviště v platnost
IČZ	<ICZ>	Identifikační číslo zařízení
Kód odbornosti	<KodOdb>	Kód odbornosti daného pracoviště
Variabilní symbol	<VarSym>	Variabilní symbol ze systému AMIS*H. pro účtování pojišťovny
AssigningAuthority	<AssigningAuthority>	Systém, ve kterém je dané pracoviště zavede
Facility	<Facility>	Zařízení, pod kterým je pracoviště vedeno
Ulice	<Ulice>	Ulice
PSČ	<PSC>	Poštovní směrovací číslo
Telefon	<Telefon>	Telefon na dané pracoviště
Základní informace	<BaseInfo>	Obsahuje datum poslední změny.

GetOrgUnitsByCostCenter

Slouží pro vyhledávání seznamu pracovišť podle identifikátoru nákladového střediska ze systému Navision, v OrgUnit vedeno jako CostCenterItem.

Odpověď poskytuje jako pole Pracovišť obsahující infromace z tabulky 31.

5 Ekonomické zhodnocení

V rámci ekonomického zhodnocená vyjádřím veškeré náklady na systém spojené s vývojem a implementací vlastního systému, následně je porovnám s časem ušetřeným řešením automatických úkolů, centrální správou oprávnění a obecnými přínosy pro organizaci.

5.1 Náklady na systém

Náklady na systém se v tomto případě rozumí práce odvedená na vývoji daného systému, která zahrnuje i počáteční analýzu, náklady na implementaci systému a náklady na podporu systému.

Tab. 31: Náklady systému [vlastní zpracování]

Činnost	Časová náročnost (člověkohodiny)	Hodinová mzda	Celkem
Vývoj	980	1 000,00 Kč	980 000,00 Kč
Implementace	320	800,00 Kč	256 000,00 Kč
Celkem	-	-	**1 236 000,00 Kč**
Podpora/Rok	100	700,00 Kč	**70 000,00 Kč**

Celková pořizovací náklady na systém tedy činí **1 236 000 Kč** a roční náklady na podporu činí **70 000 Kč/rok**. Díky využití stávajících technologií nevznikají pro potřeby implementace systému další náklady na hardware, nebo softwarové licence.

5.2 Ušetřené náklady nasazením systému

Hlavní výhodou nasazení systému pro správu identit je ušetření času spojené s realizováním automatických úkonů při nástupu a ukončení pracovního poměru. Tyto úkony zaberou správcům cca 0,2 hodiny pro jeden systém. Většina zaměstnanců má přístup do 2 systémů (někteří i více) při měsíční fluktuaci cca 100 zaměstnanců s přístupy do systémů vychází čas správců strávený správou automatizovaných činností na 480 hodin. Ty při ohodnocení **700 Kč/hod** dávají celkovou částku **336 000 Kč** ročně.

Další výhodou je zjednodušení nastavování práv, kdy úprava bezpečnostní politiky nemůže probíhat přímo pro dané uživatele, ale podle obecných kritérií jim mohou být přidělena typová pracovní místa (lékař, sestra, vedoucí pracovník). Toto ušetření času ušetří až desítky hodin pro každou změnu. Vzhledem ke zvyšujícím požadavkům na bezpečnost může takových změn proběhnout až 10 do roka. Při náročnosti 15 hodin na změnu v rámci všech systémů a počtu 5 změn do roka se správcům systému ušetří 150 hodin ročně což je **105 000 Kč**.

Při celkové úspoře nákladů **441 000 Kč/rok** a nákladech na podporu **70 000 Kč/rok** je celková roční úspora **371 000 Kč/rok** a tím pádem celková návratnost systému **3,3 roky.** Tato návratnost je pro informační systémy nadstandartní a je výrazně nižší než očekáváná životnost systému.

5.3 Přínosy nefinančního charakteru

Mezi ostatní přínosy nefinančního charakter patří mimo jiné:

- Zvýšení průhlednosti:
    - organizační struktury
    - práce s přístupy
- Zrychlení možnosti centrálně reagovat na změny v bezpečnostní politice
- Rozšíření funkcionalit integrační platformy

- Zvýšení bezpečnosti celé organizace
- Zvýšení pohodlí práce správců systému pomocí jednotného přístupu a možnosti auditu

6 ZÁVĚR

V rámci této diplomové práce jsem se zabýval návrhem informačního systému pro správu identit v organizaci, jejich životního cyklu a oprávnění. Tento systém byl navrhován pro obecné použití se přihlédnutím ke specifických požadavkům Fakultní nemocnice Brno.

Navrhované řešení splňuje obecné standardy práce s identitami a je rozdělitelné do 3 logických celků provisioning systému, adresářové struktury a systému řízení přístupů. Všechny tři části obsahují mechanismy pro audit změn a odpovídající rozhraní pro správu.

Pro provisioning systém jsou čerpána data ze zdrojových systému Navision a AMIS. Dále je jako zdrojový systém použito Active Directory pro účely delegovaného ověřování identit. V rámci provisioning systému lze nastavovat bezpečnostní politiku napříč napojenými systémy pracujícími na architektuře rolí. Dále je zde možné i nastavování individuálních oprávnění, která neodpovídají obecně platným pravidlům politiky.

Adresářová struktura, která stojí mezi provisioning systémem a systémem řízení přístupů uchovává základní informace o identitách, které jsou dalším systémům poskytovány v rámci systému řízení přístupů. Díky využití technologií integrační platformy Ensemble je zajištěna vysoká dostupnost a jednoduchá replikace.

Třetí částí řešení je systém řízení přístupů, který pomocí popsaného rozhraní poskytuje strukturované informace o uživatelích, jejich pracovních poměrech a oprávněních, ale také o organizační struktuře, kterou systém využívá a spravuje.

Pro audit každého ze tří hlavních pilířů systému je navržena struktura logů, které poskytují správci možnost dohledání původu změn v systému a zvyšují průhlednost případných nesrovnalostí.

Vlastní systém je v poslední části mé práce zhodnocen z hlediska nákladů a přínosů v podobě ušetřených nákladů a přínosů nefinančního charakteru. Dle tohoto zhodnocení se ukazuje jako pro organizaci rentabilní investice do budoucnosti.

7 SEZNAM POUŽITÝCH ZDROJŮ

[1] BASL, Josef. *Podnikové informační systémy: podnik v informační společnosti*. 2., výrazně přeprac. a rozš. vyd. Praha: Grada, 2008. ISBN 978-80-247-2279-5.

[2] SKLENÁK, Vilém. *Data, informace, znalosti a Internet*. Vyd. 1. V Praze: C.H. Beck, 2001. ISBN 80-7179-409-0.

[3] KOCH, M. *Datové a funkční modelování* (přednáška). Brno: VUT v Brně, Fakulta Podnikatelská, 2014.

[4] BRUCKNER, Tomáš. *Tvorba informačních systémů: principy, metodiky, architektury*. Praha: Grada, 2012, ISBN 978-80-247-4153-6.

[5] ISO/IEC 27001 - Information security management. *ISO – International Organization for Standardization* [online]. Geneva: International Organization for Standardization, 2014 [cit. 2019-01-17]. Dostupné z: http://www.iso.org/iso/iso27001

[6] BISHOP, Matt. *Computer security: art and science*. Boston: Addison-Wesley, c2003. ISBN 02-014-4099-7.

[7] *NGN Identity Management Framework: Recommendation Y.2720*. Paris: International Telecommunication Union, 2009.

[8] STAMP, Mark. *Information security principles and practice* [online]. Hoboken, N.J: Wiley-Interscience, 2005, s. 153-176 [cit. cit. 2016-10-5]. ISBN 9780471744191.

[9] KRHOVJÁK, Jan a Václav MATYÁŠ. Autentizace a identifikace uživatelů. *Zpravodaj ÚVT MU: bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě* [online]. Brno: Masarykova univerzita, 2011, **XVIII**(1) [cit. 2018-10-5]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/560.html#lit1.

[10] Jak je na tom Vaše heslo? ÚSTAV VÝPOČETNÍ TECHNIKY MU. *CSIRT MU* [online]. 2014 [cit. 2018-10-6]. Dostupné z: https://security.ics.muni.cz/18-Jakje-na-tom-vase-heslo.

[11] BONNEAU, Joseph, Cormac HERLEY, Frank STAJANO, Paul C. VAN OORSCHOT. *The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes*. Cambridge, 2012. Dostupné také z: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf. Technical report. University of Cambridge, Computer Laboratory.

[12] Biometrika: Basics of fingerprint recognition technology and biometric systems. BIOMETRIKA S.R.L. *Biometrika* [online]. 2012, 2015 [cit. 2018-11-17]. Dostupné z: http://www.biometrika.it/eng/wp_biointro.html.

[13] BERTINO, Elisa a Kenji TAKAHASHI. *Identity management: concepts, technologies, and systems*. Boston: Artech House, 2011. Artech House information security and privacy series. ISBN 16-080-7039-5.

[14] BALÁŽIK, Milan. Principy řízení identit. *IT SYSTEMS* [online]. 2015, (1-2) [cit. 2016-11-5]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/itsecurity/principy-rizeni-identit.htm.

[15] LÍZNER, Martin. Identity management: centrální správa uživatelských účtů. *Computerworld* [online]. Praha, 2010 [cit. 2016-11-26]. Dostupné z: http://computerworld.cz/securityworld/identity-management-centralnispravauzivatelskych-uctu-47568

[16] SEMANČÍK, Radovan a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (1. díl): Základy správy identit a přístupů. *IT SYSTEMS* [online]. 2015, (1-2) [cit. 2019-02-02]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-identity-managementu1-dil.htm.

[17] HURSTI, Jani. *Single Sign-On* [online]. Helsinki, 1997 [cit. 2016-11-24]. Dostupné z: http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/single_sign-on.html. Helsinki University of Technology, Department of Computer Science.

[18] KIRSTEN, Wolfgang. *Caché: databáze postrelačního typu a tvorba aplikací.* Brno,: CP Books, 2005. ISBN 80-251-0491-5.

[19] BRUCKNER, Tomáš, 2012. *Tvorba informačních systémů: principy, metodiky, architektury*. Praha: Grada. Management v informační společnosti. ISBN 978-80-247-4153-6.

[20] MINISTERSTVO ZDROVOTNICTVÍ ČESKÉ REPUBLIKY. *Zdraví 2020: evropská zdravotní politika*. *mzcr.cz* [online] [cit. 2019-1-18]. Dostupné z: http://www.mzcr.cz/verejne/dokumenty/ramcovy-souhrn-opatreni-zdravi-2020_8526_3016_5.html

[21] FAKUTNÍ NEMOCNICE BRNO *Výroční zpráva – Fakultní nemocnice Brno* [online] [cit. 2019-04-04] dostupné z http://www.fnbrno.cz/vyrocni-zprava/t1178

[22] ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ). *Počet a věkové složení obyvatel – vybrané území* [online]. [cit. 2016-11-03]. Dostupné z: https://vdb.czso.cz/vdbvo2/faces/cs/index.jsf?page=vystup-objekt&f=TABULKA&z=T&pvo=DEM02&katalog=30845&c=v3~3__RP2015&u=v75__VUZEMI__43__582786&str=v75&rouska=true&clsp=null#w=

[23] Legislativa | Elektronické preskripce. *Elektronické preskripce | eRecept* [online]. Copyright © SÚKL. Šrobárova 48, 100 41 Praha 10 [cit. 19.04.2019]. Dostupné z: https://www.epreskripce.cz/legislativa

[24] Co je GDPR? | GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. Dostupné z: https://www.gdpr.cz/gdpr/

[25] Evropská protipadělková směrnice a její dopad na značení léků | CODEWARE, s.r.o.. CODEWARE, s.r.o. [online]. Copyright © Codeware s.r.o, Jaromírova 37, 120 00 Praha 2, tel. [cit. 19.04.2019]. Dostupné z: http://www.codeware.cz/blog/evropska-protipadelkova-smernice-a-jeji-dopad-na-znaceni-leku

[26] *Archi: Open Source ArchiMate Modeling* [online], [cit. 2019-05-07]. Dostupné z: https://www.archimatetool.com/

8 SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

FN – Fakultní nemocnice

IS – Informační systém

CI – centrum informatiky

9 SEZNAM POUŽITÝCH TABULEK

TAB. 1: PŘÍPAD UŽITÍ [19] 28
TAB. 2:POČET A VĚKOVÉ SLOŽENÍ OBYVATEL PRO BRNO-MĚSTO.[22] 37
TAB. 3: SWOT ANALÝZA [VLASTNÍ ZPRACOVÁNÍ] 46
TAB. 4: PŘÍPAD UŽITÍ SYNCHRONIZACE PROVISIONING SYSTÉMU [VLASTNÍ ZPRACOVÁNÍ] 54
TAB. 5: PŘÍPAD UŽITÍ ZAVÁDĚNÍ BEZPEČNOSTNÍ POLITIKY [VLASTNÍ ZPRACOVÁNÍ] 55
TAB. 6: PŘÍPAD UŽITÍ NASTAVENÍ INDIVIDUÁLNÍHO OPRÁVNĚNÍ [VLASTNÍ ZPRACOVÁNÍ] 56
TAB. 7: PŘÍPAD UŽITÍ NOTIFIKACE O ZMĚNÁCH OPRÁVNĚNÍ [VLASTNÍ ZPRACOVÁNÍ] 57
TAB. 8: PŘÍPAD UŽITÍ OVĚŘENÍ IDENTITY UŽIVATELE [VLASTNÍ ZPRACOVÁNÍ] 58
TAB. 9: PŘÍPAD UŽITÍ ZÍSKÁNÍ PŘÍSTUPOVÝCH PRÁV UŽIVATELE [VLASTNÍ ZPRACOVÁNÍ] 59
TAB. 10: PŘÍPAD UŽITÍ ZÍSKÁNÍ INFORMACÍ O UŽIVATELI [VLASTNÍ ZPRACOVÁNÍ] 60
TAB. 11: PŘÍPAD UŽITÍ AUDIT ZMĚN V PROVISIONING SYSTÉMU [VLASTNÍ ZPRACOVÁNÍ] 61
TAB. 12: PŘÍPAD UŽITÍ KONTROLA STAVU SYSTÉMU [VLASTNÍ ZPRACOVÁNÍ] 62
TAB. 13: PŘÍPAD UŽITÍ KONTROLA NOTIFIKACE [VLASTNÍ ZPRACOVÁNÍ] 63
TAB. 14: PŘÍPAD UŽITÍ KONTROLA DOTAZŮ NA WEBOVÉ SLUŽBY [VLASTNÍ ZPRACOVÁNÍ] 64
TAB. 15: PŘÍPAD UŽITÍ KONTROLA STAVU SYNCHRONIZACE [VLASTNÍ ZPRACOVÁNÍ] 65
TAB. 16: PŘÍPAD UŽITÍ KONTROLA INTEGRITY DAT [VLASTNÍ ZPRACOVÁNÍ] 66
TAB. 17: ATRIBUTY ADRESÁŘOVÉ STRUKTURY [VLASTNÍ ZPRACOVÁNÍ] 72
TAB. 18: STRUKTURA INFORMACÍ SYSTÉMU NAVISION HR [VLASTNÍ ZPRACOVÁNÍ] 79
TAB. 19: STRUKTURA INFORMACÍ SYSTÉMU NAVISION ERP[VLASTNÍ ZPRACOVÁNÍ] 80
TAB. 20: POŽADAVEK PRO GETROLES [VLASTNÍ ZPRACOVÁNÍ] 81
TAB. 21: ODPOVĚĎ PRO GETROLES [VLASTNÍ ZPRACOVÁNÍ] 81
TAB. 22: STRUKTURA ELEMENTU ROLE [VLASTNÍ ZPRACOVÁNÍ] 82
TAB. 23: POŽADAVEK PRO GETEMPLOYMENTS [VLASTNÍ ZPRACOVÁNÍ] 82
TAB. 24: ODPOVĚĎ PRO GETEMPLYMENTS [VLASTNÍ ZPRACOVÁNÍ] 83
TAB. 25: STRUKTURA ELEMENTU DATA [VLASTNÍ ZPRACOVÁNÍ] 83
TAB. 26: POŽADAVEK PRO GETEMPLOYEE [VLASTNÍ ZPRACOVÁNÍ] 84
TAB. 27: ODPOVĚĎ PRO GETEMPLOYEE [VLASTNÍ ZPRACOVÁNÍ] 84
TAB. 28: INFORMACE O ZAMĚSTNANCI PRO EKONOMICKÉ SYSTÉMY [VLASTNÍ ZPRACOVÁNÍ] 84
TAB. 29: POŽADAVEK PRO SLUŽBU GETORGUNIT [VLASTNÍ ZPRACOVÁNÍ] 85
TAB. 30: ODPOVĚĎ PRO SLUŽBU GETORGUNIT [VLASTNÍ ZPRACOVÁNÍ] 85
TAB. 31: NÁKLADY SYSTÉMU [VLASTNÍ ZPRACOVÁNÍ] 88

10 SEZNAM OBRÁZKŮ

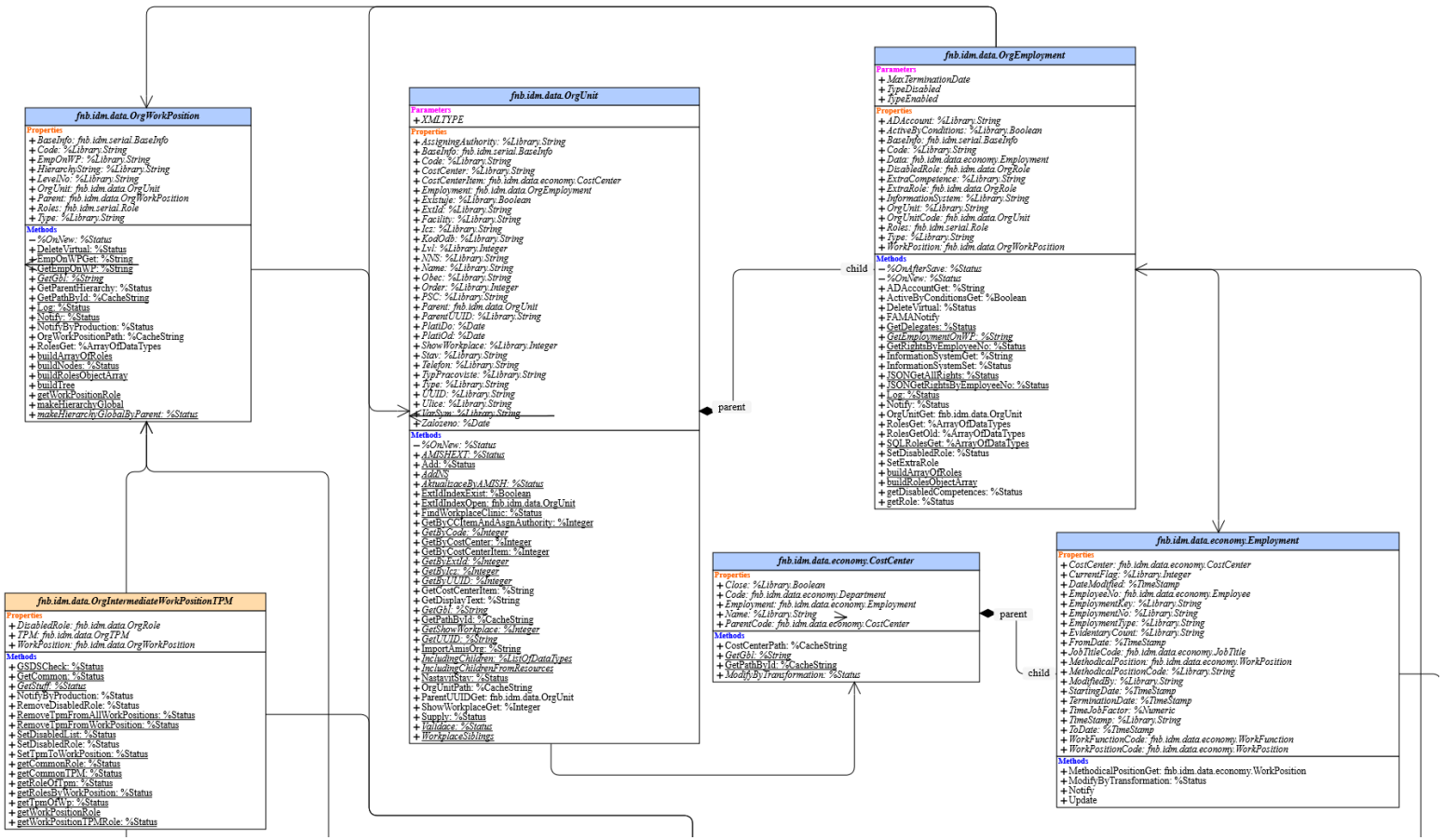
OBR. 1 UML AKTÉR [VLASTNÍ ZPRACOVÁNÍ] 27
OBR. 2 UML PŘÍPAD UŽITÍ [VLASTNÍ ZPRACOVÁNÍ] 27
OBR. 3: UML VZTAHY MEZI PŘÍPADY UŽITÍ [VLASTNÍ ZPRACOVÁNÍ] 29
OBR. 4: UML ZNÁZORNĚNÍ TŘÍDY [VLASTNÍ ZPRACOVÁNÍ] 30
OBR. 5: UML VAZBA TŘÍD ASOCIACE [VLASTNÍ ZPRACOVÁNÍ] 30
OBR. 6: UML VAZBA TŘÍD KOMPOZICE [VLASTNÍ ZPRACOVÁNÍ] 31
OBR. 7: UML SEKVENČNÍ DIAGRAM ZPRÁVY [VLASTNÍ ZPRACOVÁNÍ] 32
OBR. 8: PRVKY BUSINESS VRSTVY ARCHIMATE [VLASTNÍ ZPRACOVÁNÍ] 34
OBR. 9: PRVKY APLIKAČNÍ VRSTVY ARCHIMATE [VLASTNÍ ZPRACOVÁNÍ] 34
OBR. 10: PRVKY TECHNOLOGICKÉ VRSTVY ARCHIMATE [VLASTNÍ ZAPRACOVANÍ] 35
OBR. 11: ORGANIZAČNÍ STRUKTURA V RÁMCI NEMOCNICE [21] 41
OBR. 12: SCHÉMA IS V RÁMCI FN BRNO [VLASTNÍ ZPRACOVÁNÍ] 42
OBR. 13: ARCHITEKTURA SYSTÉMU [VLASTNÍ ZPRACOVÁNÍ] 51
OBR. 14: BUSINESS VRSTVA [VLASTNÍ ZPRACOVÁNÍ] 52
OBR. 15: PŘÍPADY UŽITÍ [VLASTNÍ ZPRACOVÁNÍ] 53
OBR. 16: APLIKAČNÍ VRSTVA [VLASTNÍ ZPRACOVÁNÍ] 67
OBR. 17: UŽIVATELSKÉ ROZHRANÍ PROVISIONING SYSTÉMU [VLASTNÍ ZPRACOVÁNÍ] 69
OBR. 18: VYHLEDÁVÁNÍ V APLIKACI [VLASTNÍ ZPRACOVÁNÍ] 70
OBR. 19: HIERARCHICKÝ SEZNAM [VLASTNÍ ZPRACOVÁNÍ] 70
OBR. 20: ZÁLOŽKY PRACOVNÍHO MÍSTA [VLASTNÍ ZPRACOVÁNÍ] 71
OBR. 21: TECHNOLOGICKÁ VRSTVA [VLASTNÍ ZPRACOVÁNÍ] 76
OBR. 22: DATOVÁ STRUKTURA EKONOMICKÝCH DAT [VLASTNÍ ZPRACOVÁNÍ] 77
OBR. 23: DATOVÁ STRUKTURA SYSTÉMU [VLASTNÍ ZPRACOVÁNÍ] 78

11 SEZNAM PŘÍLOH

Příloha č. 1: Datová struktura systému část 1 i

Příloha č. 2: Datová struktura systému část 2 ii

Příloha 1: Datová struktura systému část 1



Příloha 2: Datová struktura systému část 2